www.pwc.com/gsiss2015

Управление киберрисками во взаимосвязанном мире

Основные результаты Глобального исследования по вопросам обеспечения информационной безопасности. Перспективы на 2015 год

Январь 2015 г.

pwc

Содержание

01

Киберриски: реальная и серьезная угроза

Кибербезопасность отныне представляет собой постоянный бизнес-риск

Кибербезопасность перестала быть проблемой, которая беспокоит лишь специалистов по информационным технологиям и информационной безопасности. Инциденты в сфере кибербезопасности сказываются на деятельности высшего руководства и на решениях, принимаемых советом директоров.

Потребителям также хорошо известно об инцидентах и угрозах в сфере информационной безопасности, и это вызывает у них серьезную озабоченность. Одним словом, трудно назвать другие вопросы, относящиеся к сфере управления рисками, которые носят столь же всеобъемлющий характер, как кибербезопасность.

Сообщения в СМИ о различных инцидентах информационной безопасности стали таким же обычным делом, как прогноз погоды, и за последний год практически все отрасли во всем мире пострадали от киберугроз того или иного рода.

Ниже приводится лишь несколько примеров таких угроз. По мере того как инцидентов становится все больше, органы государственной власти принимают предупредительные меры, помогая организациям в борьбе с киберпреступностью.

К примеру, Федеральное бюро расследований США (ФБР) объявило, что уведомило 3 000 компаний (включая банки, предприятия розничной торговли и подрядчиков, работающих на оборонную промышленность) о том, что в 2013 году они стали жертвами преступлений, связанных со взломом системы кибербезопасности[1].

Следующим шагом стало официальное обвинение, выдвинутое министерством юстиции США против пяти китайских военных хакеров, в киберэкономическом шпионаже против американских компаний, работающих в атомной энергетике, металлургии и гелиоэнергетике[2]. Это был первый в истории случай, когда Соединенные Штаты обвинили государственных чиновников в экономическом шпионаже с использованием внешних кибератак; обвинения были выдвинуты в соответствии с разделом 1831 Закона об экономическом шпионаже.

Эта тенденция, скорее всего, сохранится, считает Шон Джойс, директор PwC, в свое время работавший заместителем директора ФБР. «Думаю, мы станем свидетелями того, как министерство юстиции США и ФБР будут и впредь придерживаться стратегии решительных действий, направленных против лиц, которые действуют в интересах иностранного государства и наносят значительный ущерб американской экономике», — говорит Шон Джойс.

В прошлом году был зафиксирован небывалый рост числа попыток несанкционированного доступа к компьютерным системам крупных ритейлеров. Результатом этого стало хищение данных платежных карт сотен миллионов покупателей, огромное число судебных разбирательств, а также ускоренное внедрение нового стандарта платежных карт в США. В Великобритании сотрудником компании были похищены и выложены в Интернете данные о заработной плате и банковских счетах 100 000 сотрудников сети супермаркетов[3].

Фондовые биржи тоже регулярно становятся мишенью злоумышленников. Опрос представителей 46 глобальных фондовых бирж, проведенный Международной организацией комиссий по ценным бумагам и Всемирной федерацией фондовых бирж, показал, что **более половины из них (53%)** подвергались кибератакам[8].

Сообщения о колоссальных хищениях клиентских данных также поступили из Южной Кореи, где в результате взлома системы информационной безопасности произошла утечка данных о счетах платежных карт 105 миллионов клиентов[4]. А в Вердене (Германия) представители городских властей объявили о хищении 18 миллионов адресов электронной почты, паролей и другой информации[5].

Кибератаки, которым подверглись ритейлеры, в немалой степени способствовали повышению общего уровня информированности о киберугрозах. К такому же результату привело и освещение средствами массовой информации событий, связанных с несанкционированным доступом в систему бывшего подрядчика Агентства национальной безопасности США (АНБ) Эдварда Сноудена. Сенсационные разоблачения, которые вскрыли факты организованной Соединенными Штатами электронной слежки за частными лицами, компаниями и целыми странами, также заставили многие международные компании и правительства иностранных государств пересмотреть целесообразность закупки товаров и услуг у тех американских компаний, которые могли снабжать информацией АНБ США

Другие случаи государственного шпионажа были раскрыты фирмой Symantec, специализирующейся на разработке программного обеспечения в области информационной безопасности и защиты конфиденциальных данных. Symantec обнаружила серию кибератак на компьютерные системы правительств крупных европейских стран, предпринимавшихся как минимум в течение четырех лет. С учетом того, какие именно объекты были выбраны для кибератак, а также принимая во внимание уровень сложности задействованных вредоносных программных средств, компания Symantec пришла к выводу о том, что координацией кибератак занималась группа хакеров, поддерживаемая на государственном уровне[6].

Геополитические конфликты, особенно противостояние между Россией и Украиной, вылились в целую серию взаимных кибератак, включавших обрушение и взлом правительственных веб-сайтов по обе стороны конфликта, а также привели к распространению вредоносных программ в компьютерных системах посольств.

Основными объектами кибератак по-прежнему остаются компании сектора финансовых услуг.

Кибермошенники сумели похитить через банкоматы более **45 миллионов** долларов США с зарубежных счетов двух ближневосточных банков[7].

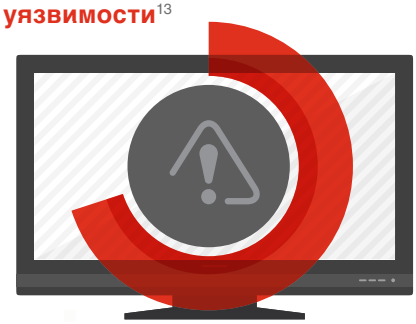
Другие важнейшие поставщики инфраструктурных услуг также подвергаются кибератакам.

Хакерская группа успешно проникла через Интернет в компьютерную систему американской государственной компании по коммунальному обслуживанию населения и взломала ее сеть системы управления. К счастью, это несанкционированное проникновение в компьютерную систему удалось остановить, прежде чем компании был нанесен какой бы то ни было ущерб[9]. В другом случае изощренные киберпреступники, действовавшие при поддержке на государственном уровне, с помощью мощных вредоносных программных средств заразили вирусом автоматизированные системы управления сотен энергетических компаний по всей территории США и Европы[10].

Одним из инцидентов года, чреватым наиболее серьезными последствиями, был дефект в протоколе OpenSSL, получивший название Heartbleed. Этот дефект протокола шифрования сказался на работе почти двух третей интернет-серверов по всему миру, включая некоторые из наиболее популярных сайтов электронной почты и социальных сетей[11].
Считается, что с использованием дефекта Heartbleed были взломаны миллионы веб-сайтов, систем онлайн-шопинга и приложений систем безопасности, а также такие программные средства, как системы обмена мгновенными сообщениями, инструменты удаленного доступа и сетевые устройства. В результате первого несанкционированного проникновения в компьютерную систему с использованием дефекта Heartbleed в одной из сетей больниц в США было похищено 4,5 миллиона медицинских карт пациентов[12].

Мы также стали свидетелями роста числа кибератак на подключаемые пользовательские устройства (например, приборы «радионяня», домашние термостаты и телевизоры), относящиеся к так называемому «Интернету вещей» – зарождающейся экосистеме устройств, обеспечивающей взаимодействие информационных, эксплуатационных и пользовательских технологий. Эти подключаемые к Интернету устройства уязвимы перед кибератаками, поскольку они не снабжены базовыми средствами защиты, что было подтверждено недавним исследованием HP Fortify on Demand.

Проанализировав десять из наиболее популярных подключаемых устройств, компания HP обнаружила, что у **70% из них имеются серьезные уязвимости**[13]



Киберриски выходят за пределы вычислительных устройств

Консалтинговая компания IOActive, занимающаяся проблемами информационной безопасности, опубликовала результаты исследования, которые наглядно демонстрируют, каким образом хакеры могут контролировать электронные устройства управления в автомобилях; в исследовании также предлагаются механизмы выявления таких атак[14].

Даже СМИ, сообщавшие о вышеупомянутых фактах несанкционированного проникновения в системы обеспечения кибербезопасности, сами оказались незащищенными от подобных атак. В прошлом году хакеры взломали компьютерные системы или нарушили нормальную работу системы безопасности некоторых из самых надежных новостных организаций мира (в том числе газет «Нью-Йорк Таймс» и «Файнэншл Таймс», телекомпании «Си-эн-эн» и информационного агентства Рейтер). Многие из наиболее резонансных кибератак были осуществлены хакерами, связанными с правительством одного из ближневосточных государств.

Безусловно, этот список ни в коем случае не является исчерпывающим. Получить точную информацию о том, какие организации пострадали от несанкционированного проникновения в компьютерную систему, будет всегда нелегко, поскольку многие из них просто не знают о том, что были атакованы хакерами или подвергаются кибератаке в настоящий момент.

Другие, возможно, не желают обнародовать известные им факты вскрытия их систем из опасения, что это может подорвать их репутацию и повлечет за собой судебные иски и расследования со стороны регулирующих органов.

Регуляторы по всему миру все чаще стараются действовать на опережение, занимаясь вопросами киберрисков.

Одним из индикаторов изменений в нормативно-правовом поле стало недавнее заявление Комиссии по ценным бумагам и биржам США (Управление инспекций и проверок соблюдения нормативно-правовых требований (OCIE)) о планах проверки более чем 50 зарегистрированных агентов, сочетающих функции брокера и дилера, и инвестиционных консультантов для определения степени их готовности к обеспечению кибербезопасности[15]. А в Сингапуре законом о защите персональных данных устанавливаются новые стандарты сбора, использования и раскрытия персональных данных.

На организации, не соблюдающие требований закона, будут налагаться штрафы в размере **1 млн сингапурских долларов (788 995 долларов США)**.[17]

В новых нормативных документах особого внимания заслуживают такие уникальные положения, как рекомендации по оформлению страхования от киберрисков и обеспечению готовности к предоставлению исчерпывающей информации обо всех инцидентах и нарушениях информационной безопасности. Директивы Комиссии по ценным бумагам дополнительно требуют от компаний внедрения процессов оценки рисков, а также более эффективного контроля за рисками взаимодействия с поставщиками, в том числе проведение независимой оценки их деятельности.

В прессе было много сообщений о том, что автомобильные компьютерные системы, зачастую подключенные друг к другу и в ряде случаев обеспечивающие беспроводную связь с внешним миром, **могут быть взломаны** с целью захвата контроля над тормозной системой, рулевым управлением и даже двигателем.

Руководители транснациональных компаний внимательно следят за подготовкой Директивы Европейского союза по защите данных, которая должна быть окончательно доработана и утверждена в 2015 году. Как ожидается, новой директивой будут предусмотрены дополнительные требования в отношении уведомления физических лиц об инцидентах несанкционированного доступа к их персональным данным. Кроме того, от организаций, занимающихся обработкой персональных данных, потребуется проведение оценки рисков и аудитов, а в случае утечки и разглашения персональных данных, организациям будут грозить более серьезные штрафы[16].

Предусмотренные Директивой ЕС по защите данных требования в части уведомления о несанкционированном доступе к персональным данным могут привести к более полному раскрытию информации об инцидентах информационной безопасности в Европе, считает Джон У. Вудс – младший, один из руководителей международной практики по предоставлению услуг в сфере обеспечения кибербезопасности юридической фирмы Baker & McKenzie LLP. «В Соединенных Штатах принятие на уровне штатов законов о необходимости уведомления об утечке или утрате персональных данных вылилось в раскрытие информации о большом числе взломов систем информационной безопасности, что в свою очередь помогло осознать всю серьезность вопросов кибербезопасности, — говорит Вудс. — Интересно посмотреть, будут ли иметь аналогичные последствия предлагаемые на уровне ЕС правовые нормы о необходимости уведомления об утечке данных. Если события будут развиваться примерно так же, как в США, думаю, мы имеем все шансы увидеть стремительный рост числа подтвержденных инцидентов (информационной безопасности) в Европе».

Мы так же видим усиление помощи со стороны государства направленное на повышение уровня кибербезопасности различных организаций.

В Соединенных Штатах, во исполнение принятого в 2013 году указа президента США о совершенствовании системы обеспечения кибербезопасности, под руководством Национального института стандартов и технологий (NIST) была разработана концепция кибербезопасности. В настоящее время отдельные компании добровольно начинают внедрение начальной версии этого стандарта для оценки и усовершенствования своих систем обеспечения кибербезопасности, а также для создания единого подхода по осуществлению разведки киберугроз и выработке тактик реагирования на них.

Попытки частного сектора усовершенствовать систему обеспечения информационной безопасности включают запуск компанией Google инициативы под названием Project Zero. Цель инициативы – повысить безопасность глобальной сети путем выявления и нейтрализации так называемых угроз «нулевого дня» (неизвестных дефектов и уязвимостей в программных кодах, которые до сих пор не были устранены), прежде чем ими смогут воспользоваться хакеры. Как отмечается в заявлении компании Google, исследователи, участвующие в Project Zero, будут работать над повышением уровня защищенности широко используемых программных средств, а также изучать мотивы и технические приемы хакеров и проводить исследования в области обеспечения эффективного мониторинга и минимизации рисков взлома систем кибербезопасности[18].

Рынок услуг в сфере кибербезопасности расширяется

Как следствие роста числа инцидентов в сфере информационной безопасности и ужесточения нормативных требований, компании и госучреждения изо всех сил стараются защитить свои данные и сети, что служит катализатором дальнейшего роста рынка решений и технологий в сфере кибербезопасности.

Согласно прогнозам исследовательской компании Gartner, которые были опубликованы газетой «Уолл-Стрит Джорнэл», в 2014 году расходы на обеспечение безопасности информационных систем в общемировом масштабе вырастут на 7,9%, достигнув 71,1 млрд долларов США. В следующем году расходы на эти цели вырастут еще на 8,2%, в результате чего в 2015 году они составят 76,9 млрд долларов США[19].

Стремительный рост числа инцидентов информационной безопасности и соответствующее освещение этих событий средствами массовой информации послужили толчком к осуществлению масштабных инвестиций венчурного капитала в компании, специализирующиеся на разработке программного обеспечения и решений в сфере кибербезопасности, а также на предоставлении услуг в этой области.

За первое полугодие 2014 года фирмы венчурного капитала инвестировали в молодые американские компании (стартапы), работающие в сфере кибербезопасности, 894 млн долларов США — почти ту же сумму, которая была инвестирована за весь 2013 год[20]. В результате этот сектор имеет все шансы зафиксировать рекордную сумму инвестиций за последние 10 лет и более. Наряду с этим рыночная капитализация некоторых фирм, работающих в сфере кибербезопасности, побила все рекорды.

Фирма FireEye, специализирующаяся на разработке решений в области обеспечения безопасности информационных сетей, проведя в 2013 году первичное публичное размещение акций (IPO), которое принесло ей 304 млн долларов США, в настоящий момент имеет рыночную капитализацию около

$4,6
млрд долларов США[21]

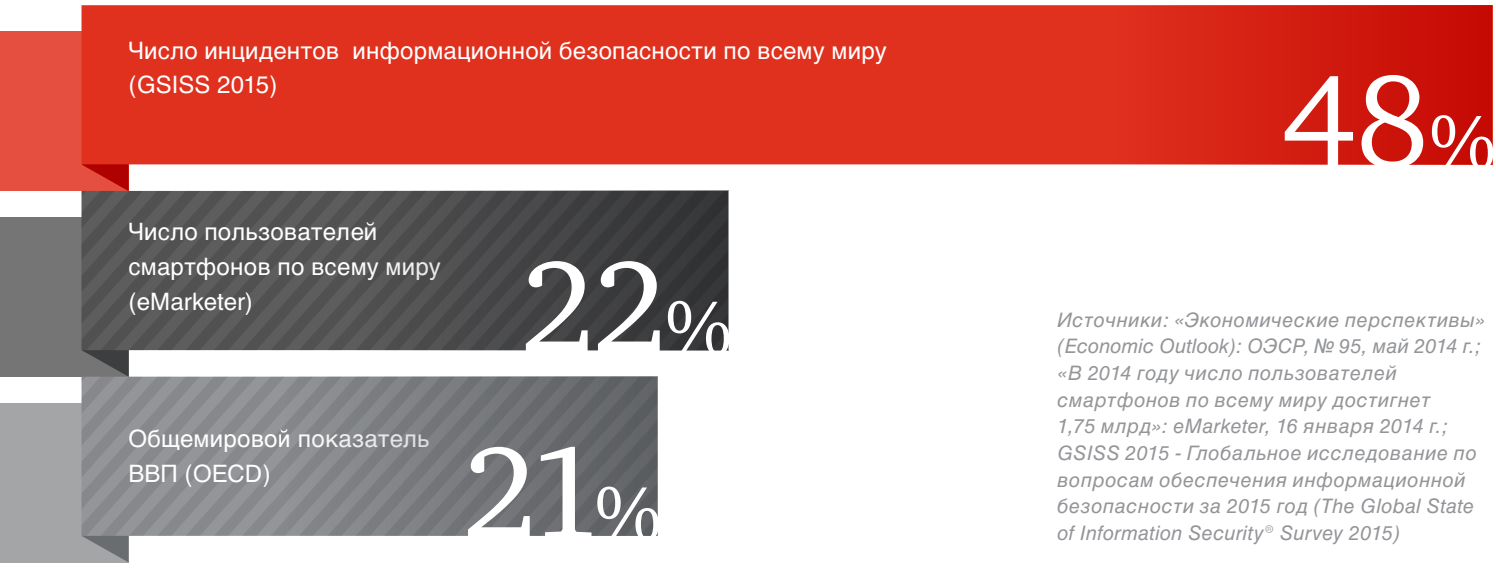
В 2012 году компания Palo Alto Networks, специализирующаяся на поставках корпоративных брандмауэров, сумела привлечь в результате IPO 260 млн долларов США. В настоящее время ее рыночная капитализация составляет примерно

$6,2
млрд долларов США[21]

Рис. 1

Темпы роста числа инцидентов информационной безопасности опережают темпы роста ВВП и рынка мобильных телефонов

Годовой прирост, 2013–2014 гг.



Источники: «Экономические перспективы» (Economic Outlook): ОЭСР, № 95, май 2014 г.; «В 2014 году число пользователей смартфонов по всему миру достигнет 1,75 млрд»: eMarketer, 16 января 2014 г.; GSISS 2015 - Глобальное исследование по вопросам обеспечения информационной безопасности за 2015 год (The Global State of Information Security® Survey 2015)

На пике бума венчурного финансирования стоимость некоторых компаний, работающих в сфере кибербезопасности, в пять-десять раз превышала их годовой доход в 2013 году.

Рынок начинает адаптироваться к новым условиям, и в последние месяцы инвестиции в компании, работающие в сфере кибербезопасности, пошли на убыль. В результате некоторые известные фирмы потеряли более половины своей прежней рыночной капитализации.

Тем не менее, есть основания полагать, что рынок программных средств, решений и услуг в сфере кибербезопасности и впредь будет расти. Причина состоит в том, что руководители компаний и члены советов директоров признают невозможность полного искоренения киберугроз, а законодательные и нормативные требования, скорее всего, будут ужесточаться.

На этом фоне, в условиях усиления рисков, ужесточения нормативных требований и активизации участников рынка, мы предлагаем вашему вниманию результаты исследования за этот год.

В Европе венчурные инвестиции в фирмы, работающие в сфере кибербезопасности, набирает обороты.

Компания C5 Capital, головной офис которой находится в Лондоне, создала фонд венчурных инвестиций, ориентированный на компании, работающие в сфере кибербезопасности, объемом

$125

млн долларов США[22]

C5 Capital также объявила об инвестициях в фирму Balabit, работающую в сфере безопасности информационных систем, в объеме

$8,0

млн долларов США[22]

Index Ventures, еще одна фирма венчурного капитала, создала фонд венчурных инвестиций в технологические стартапы в Европе, Израиле и США в общем объеме

$550

млн долларов США[23]

Прошлый год стал также годом повышенной активности по слиянию и поглощению фирм, работающих в сфере кибербезопасности.

Компания FireEye приобрела Mandiant приблизительно за

$1,0

млн долларов США

Cisco Systems приобрела Sourcefire за

$2,7

млн долларов США[24]

02

Число инцидентов и размеры причиняемого ими ущерба неуклонно растут

Продолжающийся из года в год рост числа инцидентов уже никого не удивляет

Если принять во внимание характер и число громких случаев взлома компьютерных систем и утечек конфиденциальной информации за прошедший год, то рост числа инцидентов, о которых сообщили респонденты, принявшие участие в Глобальном исследовании по вопросам обеспечения информационной безопасности за 2015 год, уже не вызывает удивления.

Результаты ежегодного опроса, в котором приняло участие более 9 700 высших должностных лиц компаний, ответственных за информационную безопасность, информационные технологии и коммерческую деятельность, показали, что общее число инцидентов в области информационной безопасности, выявленных нашими респондентами, резко возросло (на 48%) по сравнению с 2013 годом, составив в общей сложности 42,8 миллиона инцидентов. Это означает, что в среднем каждый день совершалось 117 339 кибератак.

Если анализировать ситуацию за более длительный период, то, по данным наших опросов, с 2009 года совокупный среднегодовой темп роста (CAGR) числа выявленных инцидентов информационной безопасности ежегодно увеличивался на 66%.

Впрочем, эти цифры ни в коем случае нельзя назвать окончательными: за ними скрывается лишь общее число выявленных и подтвержденных инцидентов. Как уже отмечалось, многие организации даже не подозревают о предпринятых против них кибератаках, в то время как другие организации просто не сообщают о выявленных инцидентах по причинам стратегического характера или из-за того, что в связи с какой-то конкретной кибератакой еще продолжается расследование, затрагивающее интересы национальной безопасности.

Рис. 2.

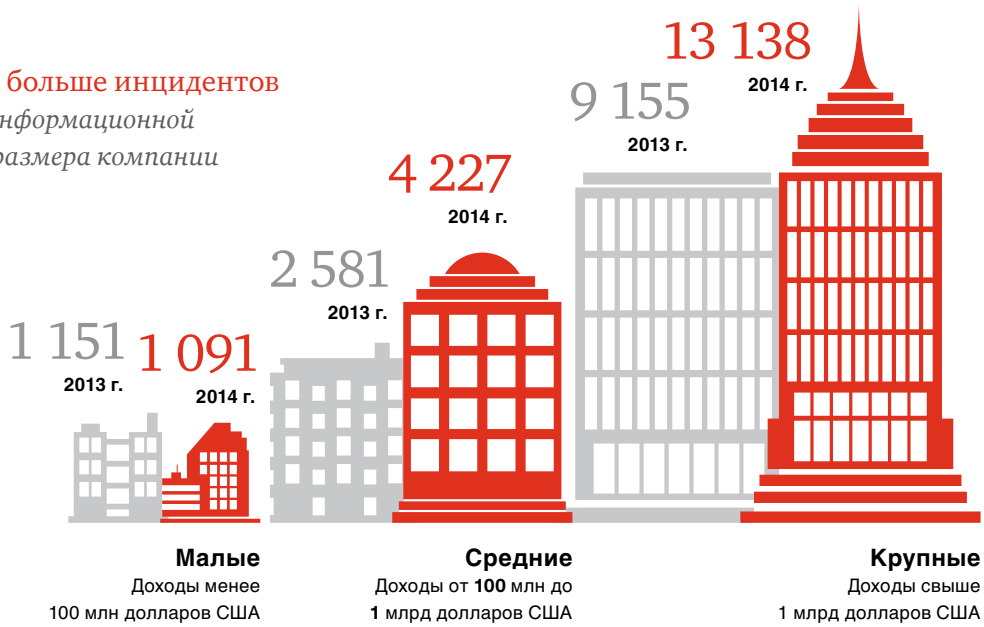
Совокупный среднегодовой прирост (CAGR) числа инцидентов информационной безопасности составляет 66%

Общее число выявленных инцидентов

Рис. 3.

Крупные компании выявляют больше инцидентов

Число выявленных инцидентов информационной безопасности в зависимости от размера компании (ее дохода)



Сегодняшние киберзлоумышленники хорошо финансируются и имеют высочайший уровень технической оснащенности, и поэтому неудивительно, что значительное количество успешных кибератак остаются необнаруженными. В частности, одна из фирм, работающих в сфере кибербезопасности, недавно подсчитала, что не менее 71% успешных попыток несанкционированного доступа в систему остаются невыявленными [25].

Что касается выявления инцидентов, одно совершенно очевидно: у крупных компаний есть преимущество перед компаниями меньшего размера.

В выборке нашего глобального исследования крупные организации (те, чей валовой годовой доход составляет не менее 1 млрд долларов США) выявили на 44% больше инцидентов по сравнению с прошлым годом. То, что крупные компании выявляют больше инцидентов, не вызывает удивления.

Киберпреступники нередко выбирают своими мишенями крупные организации, поскольку, как правило, они представляют собой настоящий кладезь ценной информации (включая документы с описанием схем совершения сделок, информацию об инновационных разработках, относящуюся к интеллектуальной собственности, и крупные объемы клиентских данных), которую можно продать или использовать для получения экономических или военных преимуществ. Кроме того, в крупных компаниях выявляется больше инцидентов, потому что, как правило, в них внедрены более эффективные процессы и технологии мониторинга и обеспечения информационной безопасности.

Другой тренд заключается, в том, что поскольку более крупные компании продолжают внедрять все более эффективные меры обеспечения информационной безопасности, киберзлоумышленники переключаются на компании среднего размера, многие из которых зачастую уделяют существенно меньше внимания защите и не имеют такого уровня зрелости в этом вопросе, как крупный бизнес. Это отчасти объясняет резкий рост (на 64%) числа инцидентов, выявленных средними по величине организациями (теми, чей доход составляет от 100 млн до 1 млрд долларов США).

В небольших организациях ситуация с выявлением случаев несанкционированного доступа в систему прямо противоположная. Компании с доходами менее 100 млн долларов США выявили в этом году на 5% меньше инцидентов, чем в предыдущем. Причины этого пока неясны, однако одно из возможных объяснений может заключаться в том, что небольшие компании вкладывают меньше средств в информационную безопасность, следствием чего может быть их неспособность эффективно выявлять инциденты и то, что они становятся более соблазнительной мишенью для кибермошенников.

Мелкие фирмы нередко считают себя слишком незначительными, чтобы привлечь внимание злоумышленников. Это опасное заблуждение. Надо отметить, что искушенные злоумышленники зачастую выбирают своей мишенью малые и средние компании, потому что видят в этом способ обосноваться во взаимосвязанных коммерческих экосистемах более крупных организаций, с которыми у этих компаний установлены партнерские отношения. Ситуацию усугубляет и то, что крупные компании обычно не уделяют должного внимания контролю за состоянием информационной безопасности своих партнеров и поставщиков.

Большинство компаний не проводят проверок деятельности и состояния информационной безопасности своих партнеров и это стало настолько распространенным явлением, что регуляторы вынуждены начать требовать обязательного проведения таких проверок. Для того чтобы пройти эти проверки и получить экономическое преимущество компании малого бизнеса могли бы отдавать на аутсорсинг функции по обеспечению своей информационной безопасности.

Крупные корпорации обладают достаточными ресурсами и знаниями для создания собственных центров обеспечения информационной безопасности с широким набором функций и возможностей, включая разведку угроз, отражение атак и расследование инцидентов. В то же время этот подход не целесообразен для мелкого бизнеса, но небольшие компании могут обеспечить наличие таких же функций кибербезопасности путем приобретения соответствующего сервиса, предоставляемого внешним поставщиком. Это позволит компании получить современные технологии и процессы защиты и обнаружения инцидентов информационной безопасности при оптимальных затратах.

Другим вариантом реагирования на киберриски является приобретение компанией соответствующей страховки.

Анализ инцидентов информационной безопасности в разных географических регионах свидетельствует о существенном росте киберпреступности в Европе, где в течение 2013 года число выявленных инцидентов **возросло на 41%**

Вполне вероятно, что Европа лидирует по числу выявленных инцидентов информационной безопасности, что подтверждается 12%-м ростом расходов на обеспечение информационной безопасности.

Это один из самых высоких показателей среди всех регионов.

В Северной Америке респонденты выявили в этом году на 11% больше инцидентов. Респонденты из Азиатско-Тихоокеанского региона, сообщившие о пятипроцентном увеличении этого показателя, судя по всему, менее сведущи в выявлении инцидентов информационной безопасности.

Южная Америка стала единственным регионом, где зафиксировано снижение числа выявленных случаев компрометации данных: количество инцидентов подобного рода здесь сократилось на 9%. Стоит отметить, что расходы на обеспечение информационной безопасности снизились в Южной Америке на 24% — это самое значительное сокращение по сравнению с другими регионами.

Рис. 4.

Бюджет на обеспечение информационной безопасности в разбивке по размеру компаний (показателю дохода)

2013–2014 гг.

Малые
Доходы менее 100 млн долларов США

Средние
Доходы от 100 млн до 1 млрд долларов США

Крупные
Доходы свыше 1 млрд долларов США

Финансовые убытки стремительно растут

По мере того как инцидентов информационной безопасности становится все больше, растут и издержки, связанные с необходимостью управлять рисками и минимизировать последствия инцидентов.

В мировом масштабе средний расчетный показатель ежегодных подтвержденных финансовых убытков, связанных с инцидентами в сфере кибербезопасности, составил 2,7 млн долларов США, что на целых 34% больше, чем в 2013 году.

В свете прошлогодних громких случаев взлома компьютерных систем и утечки конфиденциальной информации не удивляет вывод о том, что крупные убытки встречаются чаще: количество организаций, сообщивших о финансовых потерях в размере не менее 20 млн долларов США, за 2013 год увеличилось на 92%.

Рост числа инцидентов информационной безопасности, разумеется, является одной из причин такого увеличения финансовых убытков. Однако еще одно объяснение, возможно, связано с тем, что сегодняшние более изощренные кибератаки, зачастую выходят за рамки ИТ, затрагивая другие сферы бизнеса, полагает Уильям Бони, руководитель службы корпоративной информационной безопасности компании T-Mobile US.

«Финансовые убытки теперь могут включать в себя затраты на восстановительные мероприятия, связанные с мониторингом внешних последствий для клиента, а не только на восстановительные работы после операционных сбоев внутри корпоративной ИТ-инфраструктуры, ограниченной межсетевыми экранами», — комментирует Уильям Бони.

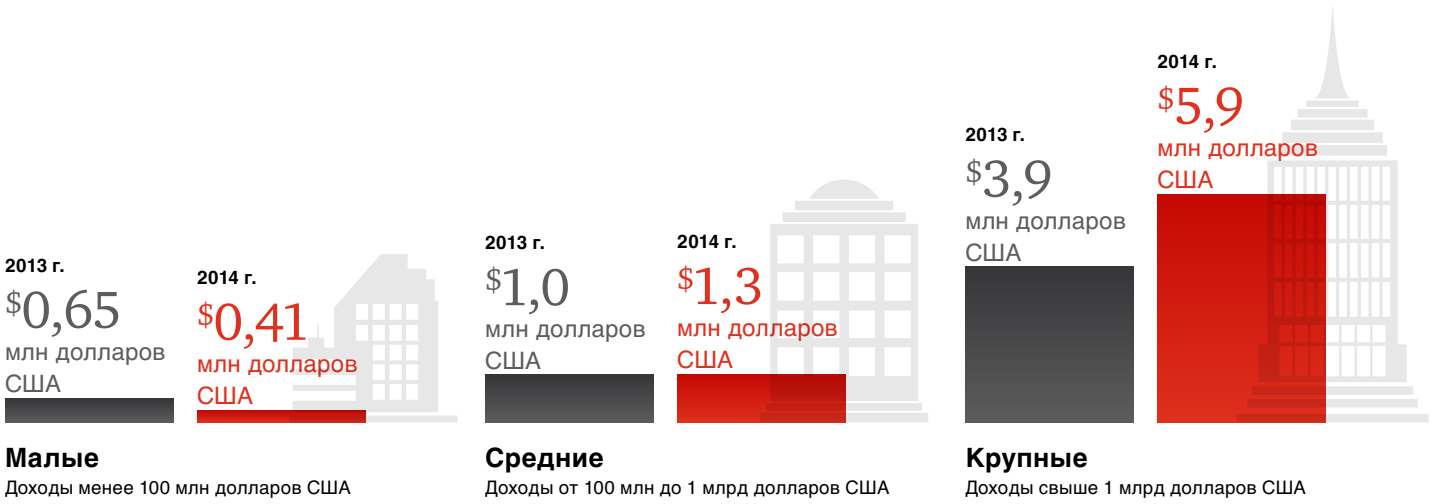
Как и в случае с общим количеством инцидентов, окончательную сумму убытков от киберпреступности в мировом масштабе узнать невозможно, поскольку о многих кибератаках просто не сообщается, а ценность некоторых видов информации, в частности интеллектуальной собственности, определить нелегко. В недавнем исследовании Центра стратегических и международных исследований обращалось внимание на трудности при оценке финансовых последствий киберпреступности. Тем не менее авторы исследования пришли к выводу о том, что размер ежегодных убытков от киберпреступности для мировой экономики составляет от 375 млрд до 575 млрд долларов США[26].

Если эта цифра кажется высокой, то следует иметь в виду, что она совершенно несопоставима с размером убытков, в которые может вылиться утрата информации, составляющей коммерческую тайну, или хищение интеллектуальной собственности. Последствия утраты информации данного вида могут быть оценены с помощью финансовых и нефинансовых показателей.

Рис. 5.

Инциденты наносят больший ущерб крупным организациям

Средний размер финансовых убытков в результате инцидентов информационной безопасности, 2013–2014 гг.



Так финансовые последствия могут включать в себя снижение доходов, сбои в работе бизнес-систем, штрафные санкции со стороны регулирующих органов и сокращение числа клиентов.

К нефинансовым последствиям можно отнести подрыв репутации компании, пиратское копирование продуктов, утечку научно-технической информации, последствия для инновационной деятельности компании, хищение продуктового дизайна или опытных образцов, незаконное копирование бизнес-процессов и производственных процессов, а также утрату такой особо важной конфиденциальной информации, как планы по осуществлению сделок слияния и поглощения и стратегия развития компании.

Исходя из подготовленной Всемирным банком оценки общемирового годового показателя ВВП за 2013 год на уровне 74,9 триллиона долларов США, размер убытка от утраты информации, составляющей коммерческую тайну, может находиться в диапазоне от **749 миллиардов до 2,2 триллиона долларов США** в год[28].

Если оценивать финансовые убытки с учетом этих факторов, их общая сумма может оказаться значительно выше по сравнению с расчетами, опирающимися на традиционные показатели.

Следует иметь в виду, что, по результатам совместного исследования Центра ответственного предпринимательства и торговли (CREATe.org) и фирмы PwC, финансовые последствия хищения коммерческих тайн составляют от 1 до 3% валового внутреннего продукта (ВВП) страны[27]. Потенциальные убытки кажутся еще более пугающими, если принять в расчет вероятность взлома систем кибербезопасности.

В докладе Всемирного экономического форума «Глобальные риски – 2014» риск кибератак был назван в числе пяти основных рисков по степени вероятности[29]. Возможность взлома системы кибербезопасности представляет собой угрозу, которую осознают многие руководители самого высокого ранга.

Почти **половина (48%)** участников опроса в рамках подготовленного PwC Всемирного обзора экономических преступлений за 2014 год (PwC's 2014 Global Economic Crime Survey) отметили, что за прошедший год уровень осознания серьезности риска киберпреступности для их организации повысился на 39% по сравнению с 2011 годом[30]. Другими словами, руководители высшего звена отдают себе отчет в том, что киберугрозы превратились в серьезную проблему в области управления рисками предприятия.

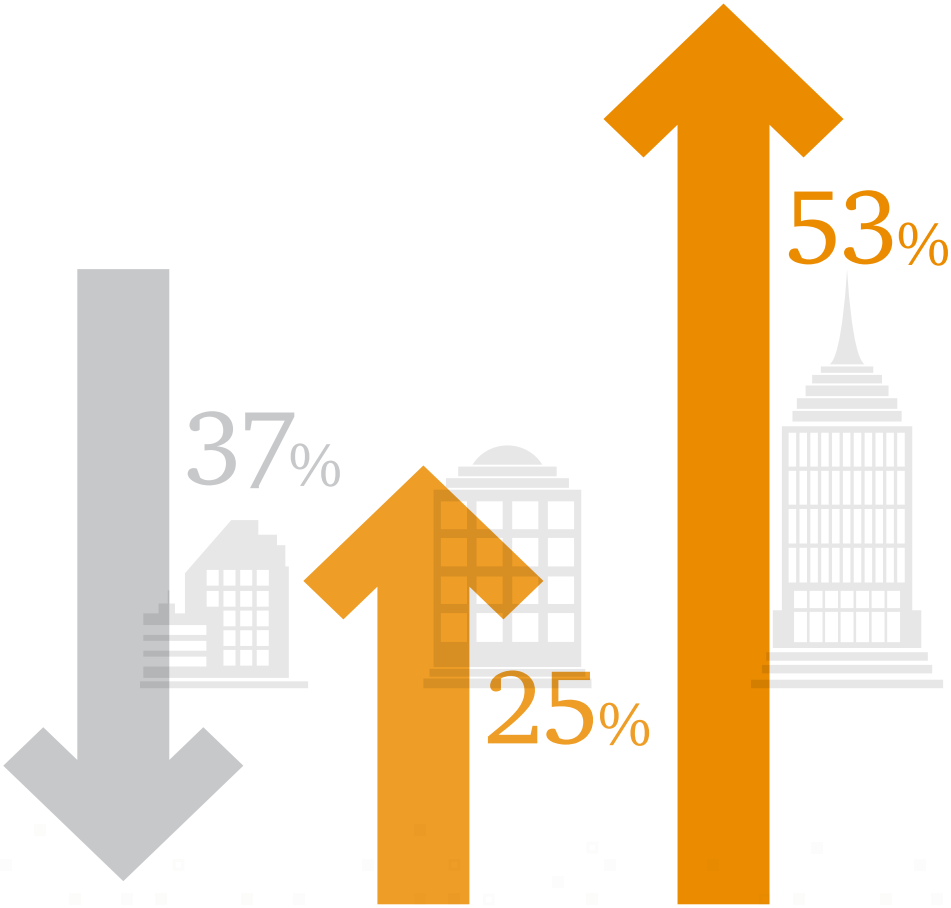
Хотя риск приобрел универсальный характер, наши специалисты, проводившие исследование в области информационной безопасности, пришли к выводу о том, что финансовые убытки, возникающие в результате инцидентов информационной безопасности, в значительной степени зависят от размера организации. Чтобы понять эту зависимость, мы проанализировали, как организации оценивают финансовые последствия инцидентов информационной безопасности. Крупные компании, как правило, выделяют больше средств на информационную безопасность и имеют более совершенную программу в этой области.

В результате у них больше шансов внедрить соответствующие бизнес-процессы и получить знания, необходимые для точного расчета финансовых убытков. А это означает, что они могут принять во внимание весь диапазон потенциальных последствий, в том числе издержки, связанные с утратой клиентского бизнеса, оплатой услуг юристов, обеспечивающих правовую защиту, судебным урегулированием, проведением судебной экспертизы и ущербом для репутации.

Кроме того, более крупные организации применяют стратегический подход к обеспечению информационной безопасности: они определяют наиболее важные активы и распределяют выделяемые средства таким образом, чтобы обеспечить защиту своих наиболее ценных данных. К тому же они, как правило, хорошо понимают риски третьих лиц и предъявляют базовые требования по безопасности к своим партнерам.

В крупных компаниях, как правило, внедрены процессы и технологии, позволяющие осуществлять активный мониторинг и анализ разведданных о киберугрозах. В случае обнаружения тех или иных аномалий их уровень готовности к отражению атак и реагированию на инциденты существенно выше, чем у небольших компаний.

Кроме того, в крупных организациях чаще существует развитая корпоративная культура информационной безопасности, которая базируется на программах повышения осведомленности персонала и соответствующих курсах обучения. В этих компаниях руководители высшего звена контролируют и гарантируют кибербезопасность на всех уровнях организации.



Небольшие компании сообщают о том, что убытки в сфере информационной безопасности в результате инцидентов фактически **сократились на 37%** по сравнению с прошлым годом, в то время как крупные компании сообщают о **резком росте (на 53%)** финансовых убытков. Организации среднего размера оказались где-то посредине: они сообщили, что убытки в сфере информационной безопасност и в результате инцидентов **выросли на 25%** по сравнению с предыдущим годом.

03

Сотрудники компаний – наиболее часто упоминаемые виновники инцидентов информационной безопасности

Внешняя разведка иностранных государств, хакеры и организованные преступные группировки — это «киберзлодеи», которыми восхищаются и которых ненавидят

Несомненно, эти субъекты действительно являются силой, с которой нужно считаться, однако так называемые инсайдеры, в частности действующие и бывшие сотрудники компании, стали самыми часто упоминаемыми виновниками киберпреступлений. Тем не менее это вовсе не означает, что все сотрудники демонстрируют злонамеренное поведение. Во многих случаях они могут стать невольными виновниками утечки информации, потеряв свои мобильные устройства или став жертвой фишинга.

10%

Процентная доля респондентов, обвиняющих действующих сотрудников своей компании, возросла на 10% по сравнению с 2013 годом.

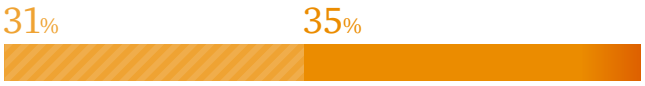
Резкий рост числа инцидентов, связанных с «инсайдерами», может повлечь за собой серьезные последствия.

В рамках нашего исследования по вопросам киберпреступности в США за 2014 год почти треть респондентов (32%) заявили, что преступления, связанные с действиями «инсайдеров», дороже обходятся компании по сравнению с инцидентами, в которых виновны «чужие»[31]. Тем не менее во многих компаниях до сих пор не внедрена программа противодействия угрозам со стороны «инсайдеров», и, соответственно, такие компании не готовы предотвращать и выявлять внутренние угрозы, а также должным образом на них реагировать.

Это риск, с которым директор PwC Шон Джойс столкнулся на личном опыте. «Опираясь на свой опыт, связанный с утечками, которые организовали [Челси] Мэннинг и Сноуден, и опыт руководства одной из ведущих инсайдерских программ в разведывательном сообществе, могу сказать, что иногда организации упускают из виду ту угрозу, которая существует внутри их собственной коммерческой экосистемы, — заявил Шон Джойс. — Последствия могут быть катастрофическими».

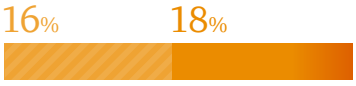
Еще одна угроза связана с тем, что, желая устранить последствия инсайдерских киберпреступлений, организации нередко пытаются обойтись своими силами. На самом деле, 75% респондентов вышеупомянутого исследования киберпреступности в США сообщили о том, что они не обращались в правоохранительные органы и не предъявляли кому-либо официальных обвинений в нарушениях, совершенных «инсайдерами».[32] Поступая таким образом, они могут подвергнуть риску другие организации, поскольку тот, кто в будущем примет этих лиц на работу, никоим образом не сможет оценить степень потенциальной угрозы с их стороны.

«Свои»



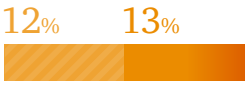
Действующие сотрудники

Бывшие сотрудники

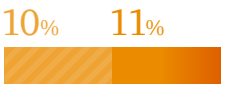


Нынешние поставщики услуг/консультанты/подрядчики

Бывшие поставщики услуг/консультанты/подрядчики



Поставщики/контрагенты



Клиенты

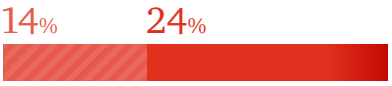
«Чужие»

Террористы

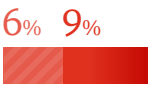
Организованная преступность

Активисты/активистские организации/«хакеры-активисты»

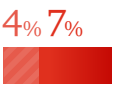
Информационные брокеры



Конкуренты



Зарубежные предприятия и организации



Иностранные государства

Служба внутренней разведки

Хакеры

Не знаю

Рис. 6.

«Свои» или «чужие»

Виновники инцидентов информационной безопасности, 2013–2014 гг.

Вместе с тем сотрудники компании — не единственный источник растущей угрозы со стороны «инсайдеров».

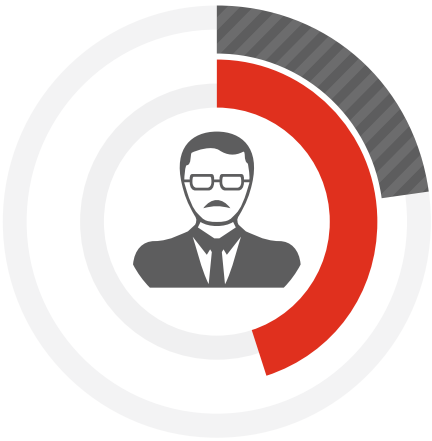
В 2014 году процентная доля инцидентов информационной безопасности, связанных с действиями нынешних и бывших поставщиков услуг, консультантов и подрядчиков, увеличилась соответственно до 18% и 15%.

То, что эта угроза слишком очевидна, чтобы ее игнорировать, стало понятно благодаря бесчисленным кибератакам на американских ритейлеров, предпринятым за прошедший год. Некоторые из успешных кибератак были совершены преступниками, получившими доступ к сетям и системам расчетных терминалов ритейлеров в местах продажи путем взлома компьютерных систем внешних поставщиков и подрядчиков.

Окрестив 2013 год «годом взлома систем ритейлеров», телекоммуникационная компания Verizon насчитала 467 успешных попыток взлома компьютерных систем ритейлеров по всему миру. В своем ежегодном отчете о результатах расследования случаев утечки данных (Data Breach Investigations Report) компания указала на то, что в 95% инцидентов, имевших место в сфере розничной торговли, основной мишенью были данные платежных карт[33].

Похоже, что 2014 год станет очередным годом беспрецедентного числа взломов компьютерных систем. Пока мы готовили этот отчет, в новостях прозвучало срочное сообщение о взломе компьютерной системы еще одного американского ритейлера, которое привело к хищению данных 56 миллионов платежных карт[34].

Анализируя ответы респондентов, представляющих компании розничного и потребительского сектора, мы пришли к выводу о заметном росте числа инцидентов, связанных с действиями **нынешних поставщиков услуг и подрядчиков (23%)**, а также **бывших партнеров (45%)**.



Если у всех этих инцидентов и есть положительная сторона, так это то, что они подстегнули индустрию платежных карт в США к переходу от существующей технологии кредитных карт с магнитной полосой к более защищенным микропроцессорным картам стандарта EMV, которые в меньшей степени подвержены угрозам утечки.

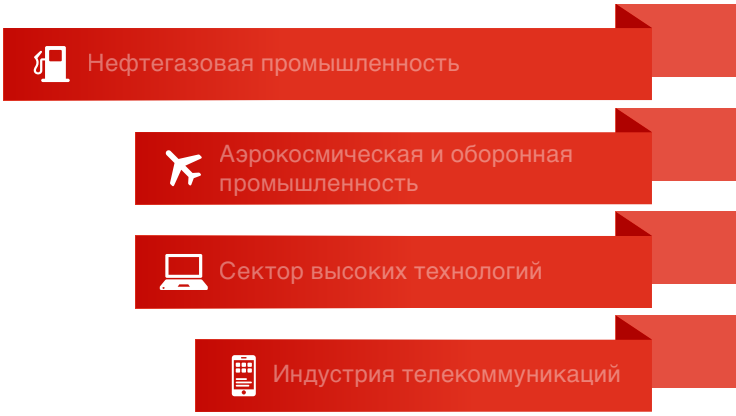
Число резонансных преступлений быстро возрастает

Киберинциденты, привлекающие к себе наибольшее внимание, а именно кибератаки со стороны иностранных государств, организованной преступности и конкурентов, по-прежнему в числе самых редких.

Однако это слабое утешение, так как результаты нашего исследования показали, что такие кибератаки входят в число угроз, растущих наиболее высокими темпами.

У многих организаций это вызывает все большие опасения, считает Лайза Дж. Comto, партнер юридической фирмы Hunton & Williams и специалист в области кибербезопасности и конфиденциальности информации. «Мне известно о колоссальном росте числа кибератак со стороны иностранных государств, которые пытаются завладеть интеллектуальной собственностью, планами проектов, данными по сделкам слияния и поглощения и научными разработками, — говорит Лайза Comto. — Рост числа кибератак со стороны организованной преступности, судя по всему, тоже бьет все рекорды, причем уровень организации и уровень развития инфраструктуры этих криминальных группировок является беспрецедентным».

Иностранные государства часто выбирают своей мишенью провайдеров и поставщиков, связанных со стратегически важными объектами инфраструктуры, стремясь присвоить интеллектуальную собственность и информацию, составляющую коммерческую тайну, для достижения собственных экономических и политических целей. Поэтому неудивительно, что инциденты с участием иностранных государств чаще всего происходят в таких секторах, как **нефтегазовая промышленность (11%), аэрокосмическая и оборонная промышленность (9%), сектор высоких технологий (9%)** и **индустрия телекоммуникаций (8%).**



Результаты опроса подтверждаются оценкой реальной ситуации. В этом году мы обнаружили, что число респондентов, сообщивших о кибератаках на них со стороны иностранных государств, увеличилось на 86%. С учетом способности враждебно настроенных иностранных государств осуществлять кибератаки, не будучи обнаруженными, мы полагаем, что объемы кибератак, по всей вероятности, занижены.

Увеличение числа инцидентов, связанных с действиями иностранных государств, отчасти может быть вызвано геополитическими событиями в Восточной Европе и на Ближнем Востоке, которые совпали по времени с ростом числа DDoS-атак (распределенных хакерских атак типа «отказ в обслуживании») и случаев использования современных шпионских программных средств.

Борьбу с киберпреступностью в лице иностранных государств осложняет то, что для большинства стран своевременный обмен оперативной информацией о киберугрозах является непростой задачей. Лишь немногие из них (в том числе США, Канада, Великобритания, Австралия и Новая Зеландия) способны осуществлять эффективный обмен информацией о кибератаках с компаниями, головные офисы которых находятся в соответствующих странах.

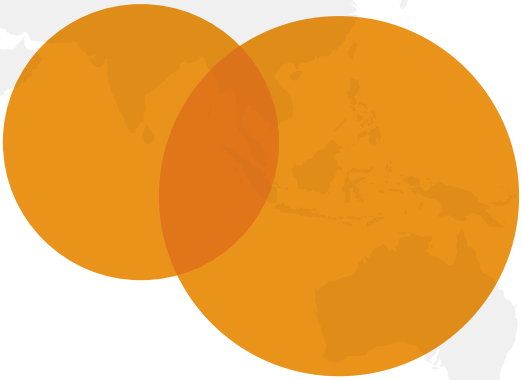
Прогресс в области совместного использования оперативных данных по информационной безопасности мог бы принести существенную экономическую пользу как странам, так и их компаниям. Более того, эффективное совместное использование данных в сочетании с исследованиями в области информационной безопасности, проводимыми частными компаниями, такими как Google, может в конечном итоге сделать киберпреступность менее прибыльным делом для злоумышленников, поскольку им придется вкладывать больше денег в новые технологии и расширение функциональных возможностей для совершения кибератак.

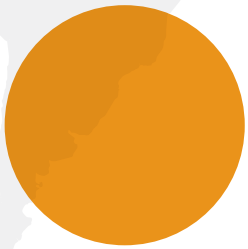
Мы также обнаружили поразительный 64% рост числа инцидентов информационной безопасности, связанных с действиями конкурентов, часть из которых может получать поддержку со стороны иностранных государств. Нигде эта проблема не стоит острее, чем в Азиатско-Тихоокеанском регионе, особенно в Китае. Почти **половина (47%)** респондентов из Китая — больше, чем в любой другой стране, — указали на конкурентов как на главных виновников инцидентов информационной безопасности.

Причиной такого роста может быть то, что компании постепенно осознают, что информация чаще всего хранится в цифровых форматах и поэтому украсть интеллектуальную собственность и коммерческую тайну проще, дешевле и быстрее, нежели делать соответствующие разработки самостоятельно. Предпринимая кибератаки, конкуренты нередко сочетают использование изощренных высокотехнологичных средств с иными «методами», такими как трудоустройство в целевую компанию, взяточничество, вымогательство и предложение дополнительного заработка. Рост киберпреступности, связанной с действиями иностранных государств и конкурентов, совпал по времени с участившимися случаями кражи интеллектуальной собственности и иной ценной информации.

В этом году число случаев кражи интеллектуальной собственности выросло по сравнению с 2013 годом на 19%. Почти каждый четвертый респондент (24%) сообщил о краже сведений, составляющих интеллектуальную собственность, в электронном формате, в том числе сведений о бизнес-процессах и накопленных в компании знаниях. Меньшее количество респондентов (15%) рассказали о случаях хищения печатных документов, содержащих стратегические бизнес-планы, информацию по сделкам и конфиденциальные финансовые данные.

В этом году 15% участников опроса назвали организованную преступность первопричиной инцидентов в сфере информационной безопасности. Это больше, чем в прошлом году, когда таких респондентов было 12%. Если говорить об отдельных регионах, то хищений, за которыми стоит организованная преступность, было особенно много в **Малайзии (35%)**, **Индии (22%)** и **Бразилии (18%)**.





О кражах интеллектуальной собственности чаще всего говорили представители аэрокосмической и оборонной отраслей, в которых коммерческая тайна может иметь стратегическое значение для национальной безопасности.

В этом году респонденты из числа представителей аэрокосмической и оборонной промышленностей сообщили о **97% увеличении числа** случаев кражи документов, содержащих сведения, относящиеся к интеллектуальной собственности, и о 66% росте числа успешных атак, приведших к хищению интеллектуальной собственности в электронном формате — это намного больше, чем в любой другой отрасли.

Растет и число успешных атак со стороны организованной киберпреступности.

Организованные преступные группировки, как правило, руководствуются стремлением к финансовой выгоде. Благодаря одной успешной кибератаке можно заполучить сведения о реквизитах миллионов платежных карт, которые можно быстро монетизировать.

Помимо данных кредитных и дебетовых карт, преступники все чаще пытаются похитить данные, содержащиеся в медицинских картах пациентов, или другие персональные данные, имеющие большую ценность в преступной среде перекупщиков информации.

В одних только Соединенных Штатах, по информации Бюро судебной статистики США, финансовые убытки, причиненные в 2012 году в результате кражи и незаконного использования персональных данных, включающих сведения о платежных картах, банковских счетах и личной жизни, составили в общей сложности 24,7 млрд долларов США[35]. Недавнее хищение учетных данных более чем миллиарда пользователей, совершенное одной из организованных преступных группировок, служит наглядным доказательством того, что масштабы кибератак такого рода растут.

В ответ на это правоохранительные органы по всему миру начинают объединять усилия в борьбе с организованной преступностью, считает Джон У. Вудс – младший, юрист, специализирующийся в области кибербезопасности. «На международном уровне все чаще признается необходимость более согласованных усилий правоохранительных органов по выявлению инцидентов, вызванных действиями организованной киберпреступности, — говорит он. — Думаю, в ближайшие годы этот процесс ускорится благодаря работе таких организаций, как Интерпол».

Внутренняя разведка: новый источник беспокойства

Благодаря раскрытию фактов электронной слежки со стороны государственных служб, которые опубликовал Эдвард Сноуден, в число источников киберугроз вошли службы внутренней разведки.

В результате связанных со Сноуденом утечек секретной информации, отношение стран, компаний и общества в целом к внутренним разведслужбам становится все более скептическим. Они также обеспокоены потенциальным воздействием слежки на конфиденциальность персональных данных и безопасность в целом.

Сенсационный характер разоблачений Сноудена стал причиной существенного повышения уровня осведомленности и обеспокоенности топ-менеджеров. Они поднимают вопросы не только о допустимости слежки со стороны государства, но и о деятельности телекоммуникационных и технологических компаний, которые могут предоставить правительству скрытый доступ к клиентским данным.

В общемировом масштабе 59% респондентов сообщили, что руководители их организаций обеспокоены фактами слежки со стороны государственных служб. Уровень обеспокоенности заметно выше в **Китае (93%)**, **Индии (83%)** и **Бразилии (77%)**.

Эта озабоченность может иметь весьма серьезные последствия для некоторых телекоммуникационных и высокотехнологических провайдеров. Европейские и особенно американские компании традиционно занимали доминирующее положение на рынке телекоммуникаций и корпоративного сетевого оборудования. Однако на рынок постепенно проникают азиатские компании, причем после того как стало известно, что правительство Соединенных Штатов собирало конфиденциальную информацию через некоторые местные технологические и телекоммуникационные фирмы, их перспективы выглядят более радужными.

В результате, в некоторых странах коммерческие компании пересматривают свое решение о закупках оборудования у определенных производителей. На самом деле, 42% респондентов сказали, что вопрос закупки товаров и услуг, производимых в определенных странах изучается, а 29% участников опроса сообщили, что они снизили объемы закупок товаров и услуг из некоторых стран.

«Эффект Сноудена», который помог потребителям понять концепцию аналитики «больших данных», стал тревожным сигналом и для отдельных граждан. По сути дела, разоблачения Сноудена и распространение «больших данных» повысили статус проблемы неприкосновенности личной жизни до уровня дебатов с участием широких слоев населения. Белый дом отреагировал публикацией в этом году двух резонансных официальных документов, посвященных влиянию «больших данных» на конфиденциальность пользовательской информации. В этих правительственных исследованиях особо подчеркивается значение интеграции стратегии безопасности «больших данных» и стратегии защиты персональных данных потребителей для защиты информации и получения конкурентных преимуществ[36].

Что больше всего беспокоит руководителей компаний? Конфиденциальность персональных данных, потенциальные юридические риски и утрата интеллектуальной собственности.

04

Число инцидентов растет, а расходы на обеспечение информационной безопасности сокращаются

Организации, несомненно, обеспокоены ростом уровня киберпреступности.

Почти половина (48%) участников опроса, проведенного PwC в рамках подготовки Всемирного обзора экономических преступлений за 2014 год (PwC's 2014 Global Economic Crime Survey), отмечают, что за прошедший год у них сформировалось более полное представление о риске киберпреступности. Это на 39% больше, чем в 2011 году[37].

В то же время, согласно результатам Ежегодного опроса руководителей компаний, проведенного PwC в 2014 году, киберугрозы, в том числе безопасность данных, вызывают обеспокоенность у 48% руководителей международных компаний[38].

Как показывает проведенное нами исследование, несмотря на возросшую обеспокоенность руководителей компаний, в 2014 году во всем мире было выделено на 4% меньше средств на обеспечение информационной безопасности, чем в 2013 году. Фактически за последние пять лет доля расходов на информационную безопасность в ИТ-бюджете ни разу не превышала 4%.

Лайза Сотто отмечает: «Информационная безопасность – это не вопрос ИТ, а проблема, лежащая в плоскости управления рисками. Информационную безопасность необходимо выделить в самостоятельную функцию с отдельной структурой управления и отдельным бюджетом, с тем чтобы на решение задачи обеспечения информационной безопасности выделялись соответствующие ресурсы. Подотчетность руководителя информационной безопасности главе ИТ-службы – это пережиток прошлого».

Но независимо от того, перед кем отчитывается служба информационной безопасности, кажется нелогичным, что по мере роста количества угроз и причиняемого материального ущерба организации не начинают вкладывать больше средств в инициативы по обеспечению безопасности. Сведения о сокращении расходов на информационную безопасность вызывают недоумение еще и потому, что, по прогнозам исследовательской компании Gartner, в 2014 году они должны были вырасти на 7,9%[39].

Проанализировав объемы вложенных средств, отраженные в нашем прошлогоднем исследовании, мы нашли объяснение замедлению темпов роста расходов. В 2013 году организации сообщили о весьма существенном увеличении расходов по сравнению с 2012 годом: инвестиции в ИТ выросли на 40%, а расходы на безопасность еще больше – на 51%. Есть основания полагать, что в этом году нашим респондентам оказалось не под силу продолжать наращивать инвестиции такими же ускоренными темпами.

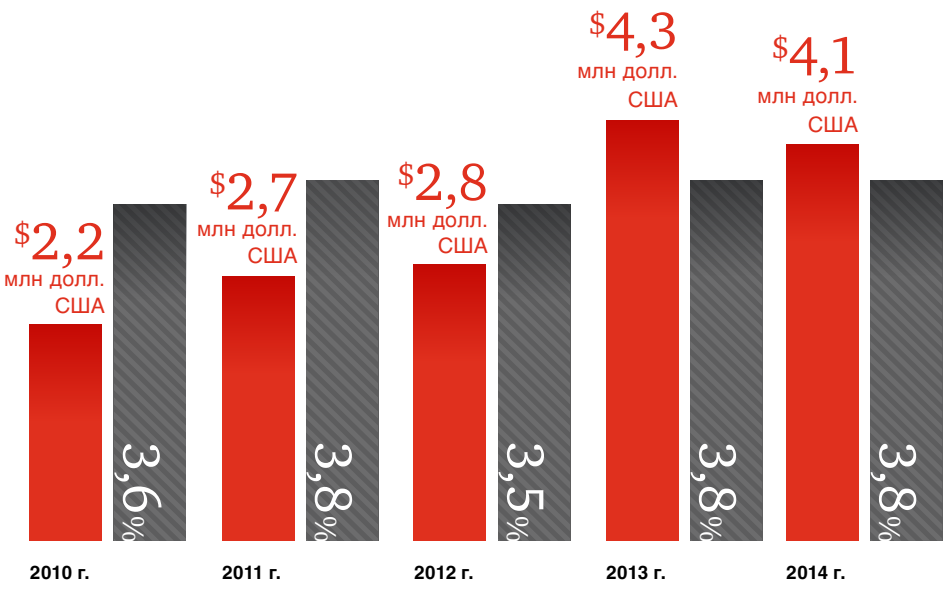


Рис. 7.

В целом отмечается незначительное сокращение среднего бюджета на обеспечение информационной безопасности, что знаменует собой изменение тренда трех последних лет.

Средний бюджет на информационную безопасность опустился до отметки 4,1 миллиона долларов США, что на 4% меньше прошлогоднего значения. Расходы на безопасность по-прежнему находятся на уровне всего лишь 3,8% от общего ИТ-бюджета.

Текущую ситуацию с бюджетами проясняет взаимосвязь между инвестициями в безопасность и размером компаний.

В этом году 20% снижение инвестиций в безопасность по сравнению с 2013 годом отмечается в компаниях с выручкой менее 100 миллионов долларов США, при этом компании среднего и крупного размера, наоборот, заявляют о 5% увеличении расходов на безопасность.

По мнению Уильяма Бони (T-Mobile), это существенный объем средств. «Одним из переменных параметров является нежелание увеличивать расходы в период нестабильности экономики, – отмечает Уильям Бони. – Полагаю, что 5% рост свидетельствует о достаточно существенном уровне внимания, с учетом того, что компании держат на голодном пайке другие корпоративные направления и хотят сохранить жесткий контроль расходов».

Помимо прочего, сложившаяся ситуация может быть обусловлена тем, что за счет использования более целенаправленных методов обеспечения безопасности организациям удалось стратегически оптимизировать свои расходы. «Думаю, что мы на пути к радикальному пересмотру своих расходов на информационную безопасность, – говорит Фернандо Камаротти, директор по информационной безопасности международной металлургической и горнодобывающей компании Vale со штаб-квартирой в Рио-де-Жанейро. – Большие и дорогостоящие проекты в прошлом были нацелены на защиту всего объема данных, но сейчас никто не считает такой подход эффективным. В дополнение к традиционным контролям информационной безопасности на уровне всей компании мы постарались найти места, где хранится конфиденциальная информация, которую необходимо защищать тщательнее. Если это сделать, то можно добиться более эффективного и рационального использования средств на обеспечение безопасности».

На фоне сокращения расходов в небольших компаниях, возникает вопрос: неужели проблема кибербезопасности не волнует их больше? С уверенностью ответить на этот вопрос нельзя, но мы, конечно же, надеемся, что это не так.

Как уже говорилось выше, небольшие коммерческие предприятия зачастую придерживаются той точки зрения, что они слишком малозначительны, чтобы заинтересовать серьезных хакеров и организованные преступные группировки. Может быть, причина кроется в том, что повышение уровня рисков наряду с изобилием решений по обеспечению безопасности привело к «аналитическому параличу», и мелкие фирмы просто неспособны принимать решения и действовать.

Это может быть и проявлением дополнительной нагрузки, отмечает юрист по вопросам кибербезопасности Лайза Сотто. «Проблема обеспечения кибербезопасности вырастает до огромных размеров, особенно для небольших компаний, в которых функцию информационной безопасности выполняют лица, не имеющие необходимой квалификации или не получившие необходимого образования», – говорит Л. Сотто.

Существует также вероятность того, что по причине нынешнего дефицита опытных специалистов в области безопасности самые высококвалифицированные кандидаты пойдут в более крупные организации с массивными бюджетами.

Что касается более крупных компаний, ограниченный рост их расходов на безопасность может объясняться тем, что на фоне нестабильности глобальной экономики корпорации все чаще идут по пути накопления денежных средств, откладывая их в большем объеме и сокращая при этом статьи расходов на ИТ и безопасность. Но на некоторые направления компании все же находят средства. Среди таких направлений можно в первую очередь выделить научные исследования и разработки.

В 2013 году 1 000 компаний, занимающих первые места по объемам расходов на НИОКР, в течение года в совокупности потратили на эти цели рекордные **638 миллиардов долларов США**, что на 6% больше, чем в предыдущем году[40].

Мы также полагаем, что многие компании не до конца понимают, сколько средств нужно выделять на безопасность и как рассчитать отдачу от инвестиций, включенных в смету расходов на безопасность. Частично это обусловлено отсутствием точных данных по текущим рискам безопасности, на которые можно было бы полагаться при разработке стратегии затрат на безопасность.

Кроме того, похоже, что трудности с обеспечением необходимого финансирования систем безопасности возникают у многих компаний еще и потому, что только у 40% из них решения по бюджету на безопасность принимаются при участии совета директоров. Мы также узнали от опрошенных, что многие топ-менеджеры и члены совета директоров зачастую не могут разобраться в том, как работают технологии обеспечения безопасности, и выявить соответствующие тактические риски.

Если проанализировать инвестиции в безопасность в разбивке по отраслям, то можно увидеть, что за редкими исключениями расходы сокращаются в большинстве секторов.

Так, например, в то время как доходы и расходы предприятий авиастроения увеличиваются, расходы на оборону в развивающихся странах падают. Частично это справедливо и для США после вывода войск из Афганистана и Ирака и последовавшего за этим сокращения оборонного бюджета. И хотя снижение расходов в секторе розничной торговли и производства потребительских товаров может показаться странным, если принять во внимание многочисленные зарегистрированные случаи нарушения систем защиты, то все равно следует помнить о том, что бюджеты на безопасность на 2014 год могли быть сформированы за год до того, как об этих инцидентах было объявлено.

Резкое сокращение бюджетов на информационную безопасность наблюдается в **аэрокосмической и оборонной промышленности (– 25%)**, **секторе высоких технологий (–21%)**, **автомобилестроении (– 16%)** и **секторе розничной торговли и производства потребительских товаров (–15%)**. В некоторых секторах это падение обусловлено конъюнктурой рынка в целом.

«Как правило, директор по информационной безопасности или финансовый директор принимает решение о выделении средств, если есть документальное подтверждение того, что та или иная проблема может стать причиной реального ущерба, – отмечает Уильям Бони (T-Mobile). – В отсутствие такого подтверждения дать количественную оценку последствий появления новых технологий и неизвестных угроз для бизнеса чрезвычайно сложно. Нужно с большой осмотрительностью подходить даже к самым незначительным суммам, выделяемым на информационную безопасность».

Среди отраслей, где отмечен наиболее существенный рост расходов на безопасность, – сфера здравоохранения и медицинского страхования (66%), нефтегазовая отрасль (15%) и топливно-энергетический комплекс (9%). Особенно существенным, но, несомненно, оправданным с учетом текущих рисков и тенденций является увеличение выделяемых на безопасность средств в сфере здравоохранения и медицинского страхования. В этом году организации сферы здравоохранения и медицинского страхования отчитались о 60-процентном росте зарегистрированных инцидентов и беспрецедентном увеличении финансовых потерь по сравнению с 2013 годом (282%).

Причина такого всплеска преступности и резкого роста размера финансовых потерь, возможно, кроется в том, что злоумышленники выбирают в качестве мишени организации сферы здравоохранения и медицинского страхования из-за имеющихся в их распоряжении данных о состоянии здоровья пациентов, с учетом того, что эти данные все больше возрастают в цене. Медицинская карта зачастую содержит целый комплект информации (финансовой, медицинской, семейной и личной), которую можно использовать для формирования полного досье на того или иного человека.

Полный комплект похищенных персональных данных со всеми сведениями о медицинской страховке может стоить на черном рынке сотни или даже тысячу долларов США, при этом одни лишь реквизиты медицинской страховки могут быть проданы за 20 долларов США. Для сравнения: украденные данные о платежных картах, как правило, продаются за 1 доллар США за карту.[41]

Черные рынки похищенных данных увеличивают свой объем и полноту данных.

По данным RAND Corporation, несмотря на то что точное количество веб-сайтов, занимающихся продажей краденых данных, неизвестно, круг злоумышленников, которые принимают участие в этих тайных сделках, скорее всего, будет расширяться, потому что участвовать в них становится все проще[42]. От части это объясняется тем, что нынешний черный рынок использует все больше веб-сайтов, форумов и чатов, на которых можно осуществить сделку купли-продажи.

Организации сферы здравоохранения и медицинского страхования могут наращивать инвестиции в безопасность, чтобы подготовиться к применению персональных устройств мониторинга и контроля состояния здоровья, а также к бурному росту объема данных, которым будет сопровождаться развитие «Интернета вещей». И действительно, для организаций сферы здравоохранения и медицинского страхования «Интернет вещей» уже не является чем-то фантастическим, а сопутствующие ему риски перешли из разряда теоретических в реальные.

Обратите внимание на то, что почти половина (47%) респондентов из числа организаций сферы здравоохранения и медицинского страхования утверждают, что уже интегрировали в свою экосистему ИТ-технологии, предназначенные для потребителей, такие как портативные устройства для контроля за состоянием здоровья, или технологии, обеспечивающие автоматизацию процессов, например автоматизированные системы выдачи медицинских препаратов.

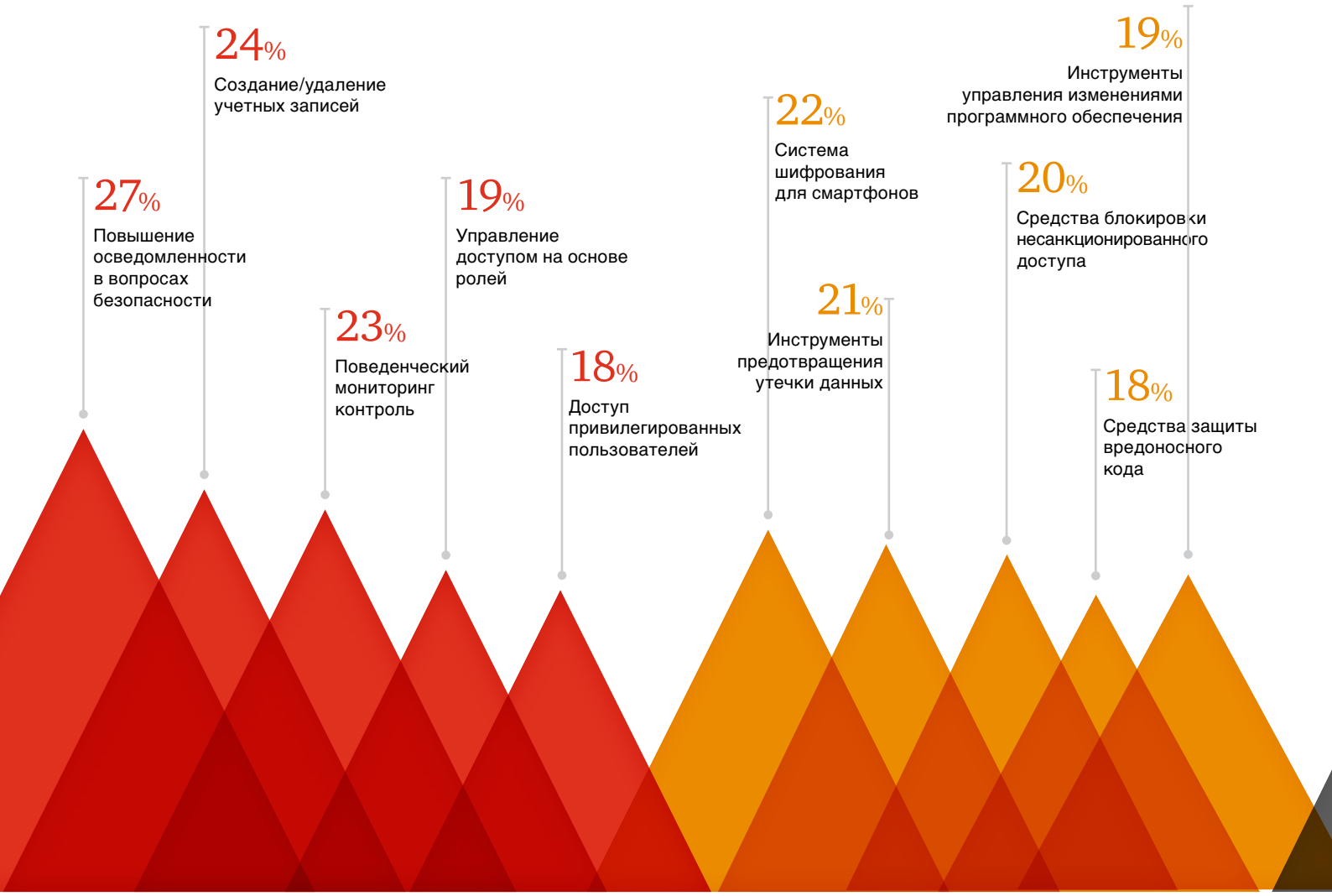
В то же время они пока не успели обеспечить безопасность этих подключаемых устройств.

Немногим **более трети (34%)** опрошенных связались с производителями устройств, чтобы разобраться в вопросах функциональности оборудования с точки зрения обеспечения безопасности и понять сопутствующие риски, и **58%** выполнили оценку рисков, связанных с указанными устройствами или технологиями. Средства контроля безопасности этих устройств внедрили только **53%** респондентов.

Рис. 8.

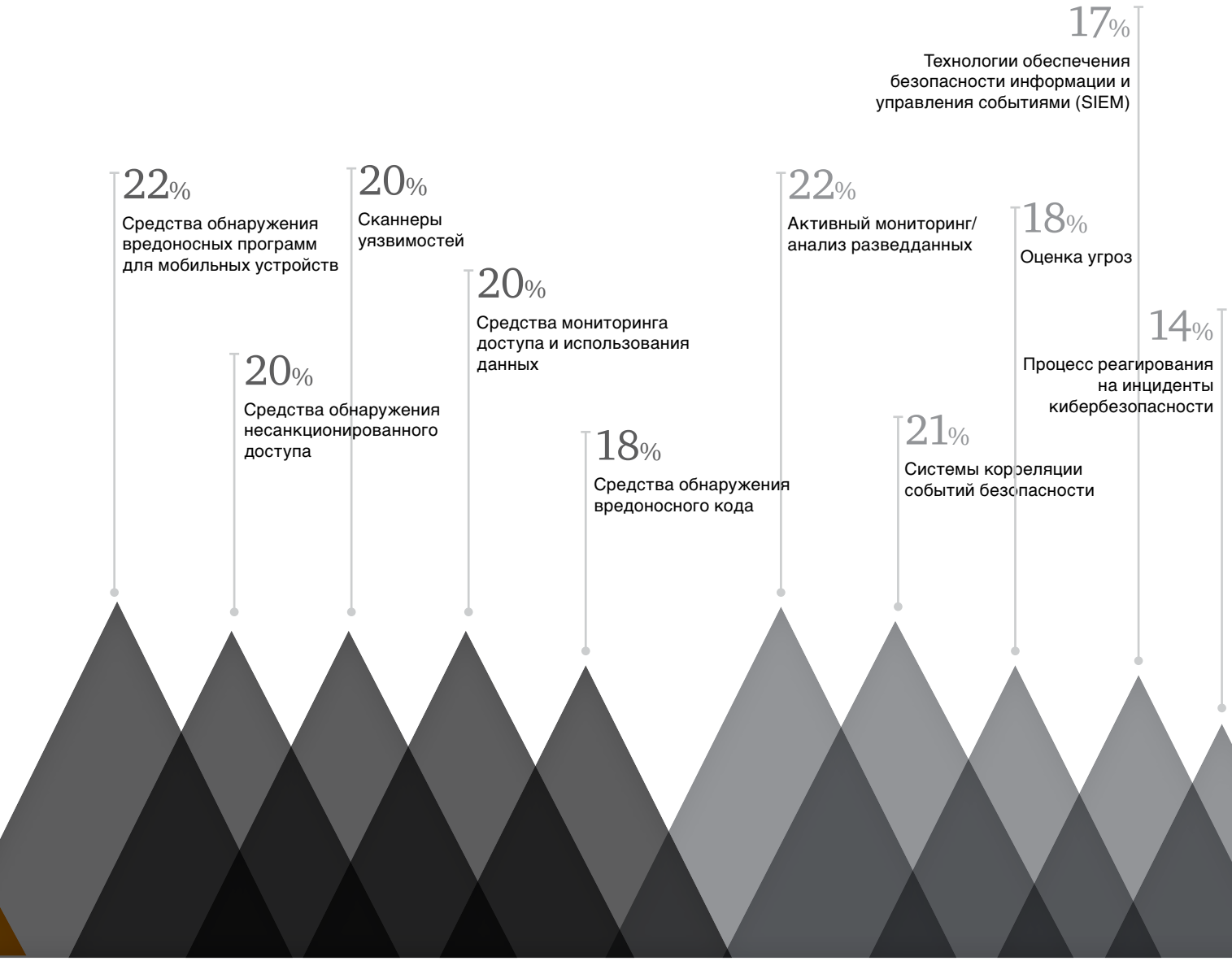
Основные статьи расходов на следующий год

Профилактика, защита, обнаружение, реагирование



Профилактика

Защита



Обнаружение

Реагирование

05

Смена фундаментальных основ обеспечения информационной безопасности

Методы защиты информации должны поспевать за постоянно эволюционирующими угрозами и требованиями в области информационной безопасности.

Для решения этой задачи необходимы инвестиции в правильно отобранные процессы и технологии, обеспечивающие предупреждение и обнаружение рисков безопасности, защиту от их воздействия и реагирование на них. Многие организации на это не способны.

Принимая во внимание тот факт, что в рамках современной взаимосвязанной бизнес-экосистемы генерируется все больше данных, объемы которых растут в геометрической прогрессии, и идет обмен этими данными с партнерами по бизнесу и поставщиками, особое внимание нужно уделять внутренним регламентам по работе с третьими сторонами, а также процедурам проверки своих контрагентов. В сложившейся ситуации не может не вызывать беспокойства тот факт, что по результатам прошлого года в ряде весьма важных областей наблюдается ослабление контроля за безопасностью при работе с третьими сторонами, даже несмотря на то что число инцидентов по вине этих «инсайдеров» растет.

«Мы считаем, что внешние поставщики представляют собой чрезвычайно существенный источник киберриска, – отмечает Лайза Сотто. – Крепость можно укрепить всевозможными фортификационными сооружениями и вырыть вокруг нее ров с водой, но если поставщики могут проникнуть внутрь по спущенному мосту, все укрепления бесполезны».

По мнению Сотто, при проведении проверок третьих лиц организации должны руководствоваться тремя основными принципами: принятие соответствующих мер защиты в отношении поставщиков, чтобы быть уверенными в том, что они способны обеспечить сохранность информации, активная реализация мер правовой защиты и постоянный мониторинг информационной безопасности третьих сторон.

Многие респонденты пока не соответствуют этим критериям. Так, например, оценку рисков, связанных со сторонними поставщиками, проводят только 50% респондентов (в 2013 году этот показатель составлял 53%) и всего 50% участников исследования провели инвентаризацию всех третьих лиц, имеющих доступ к персональным данным клиентов и сотрудников. Всего лишь немногим более половины (54%) респондентов имеют документально оформленную политику, обязывающую третьих лиц соблюдать установленные ими требования к защите персональных данных (в 2013 году этот показатель составлял 58%).

Рис. 9

Неспособность поспевать за угрозами в сфере информационной безопасности

Профилактика, защита, обнаружение, реагирование

В этом году наблюдается сокращение числа респондентов, у которых имеются программы повышения осведомленности сотрудников о различных аспектах обеспечения безопасности (с **60%** до **51%**). Несколько выше доля респондентов (**57%**), заявивших о том, что они требуют от своих сотрудников обязательного прохождения обучения по защите персональных данных.

Обучение и информирование персонала являются неотъемлемыми элементами любой программы, потому что зачастую самым слабым звеном в цепочке обеспечения безопасности оказывается человек. Нередко причиной разрыва звеньев цепи является неумение организаций взаимодействовать со своими сотрудниками и обеспечивать их осведомленность путем проведения соответствующих обучений.

Задумайтесь над тем, что 84% руководителей компаний уверены в том, что смогут достичь поставленных стратегических целей, но только 41% полагают, что их сотрудники разбираются в стратегии достаточно хорошо, чтобы принимать правильные решения на ее основе[43].

Признают важность обучения сотрудников и принимают соответствующие меры чаще всего в крупных организациях. Согласно результатам нашего исследования, так поступают 58% больших компаний в сравнении с 47% мелких фирм.

Программы обучения персонала по вопросам безопасности получили наибольшее распространение в Северной Америке и Азиатско-Тихоокеанском регионе. Бóльшую готовность к проведению подобных обучающих программ демонстрируют организации сферы здравоохранения, предприятия промышленного сектора и организации сектора финансовых услуг.

Для того чтобы обеспечить необходимый уровень осведомленности сотрудников о различных аспектах безопасности, необходимы взаимодействие в рамках всей организации по вертикали сверху вниз, а также поддержка на всех уровнях управленческой структуры. Об этой тактике зачастую забывают. Лишь 49% респондентов сказали, что в их организации сформирована рабочая группа с участием представителей всех заинтересованных служб, которая регулярно встречается для обсуждения вопросов обеспечения информационной безопасности, координации усилий в этой области и надлежащего информирования сотрудников организации. Кроме того, в решении этой задачи должен принимать непосредственное участие совет директоров и высшее руководство.

Гэри Хейз, ИТ-директор компании CenterPoint Energy (базирующееся в Хьюстоне предприятие коммунальных услуг, занимается поставками электроэнергии и природного газа), отмечает, что, для того чтобы обеспечить требуемый уровень осведомленности сотрудников о различных аспектах безопасности, необходимо соответствующее финансирование. Но, возможно, еще важнее стремление перейти на более высокий уровень развития. «Одного лишь наращивания инвестиций недостаточно, – добавляет он. – Ваша организация, ваш персонал и используемые технологии должны развиваться и выходить на более высокий уровень, и игнорирование этой задачи может стать более серьезным препятствием, чем дефицит капитала».

Ответственность за управление киберрисками должно взять на себя руководство компании. Кроме того, оно должно объяснить совету директоров каким образом организация будет защищаться от киберрисков и реагировать на них.

Обрушившийся на нас в прошедшем году шквал инцидентов заставил заговорить об участии советов директоров в решении задачи обеспечения безопасности. Но, несмотря на все разговоры, организации так и не добились включения вопросов безопасности в повестку дня заседаний советов директоров.

Мы знаем об этом, потому что мы спросили: об активном участии советов директоров в реализации общей стратегии безопасности и их вовлеченности в процесс разработки политики информационной безопасности сообщили только 42% и 36% респондентов соответственно. Всего лишь 25% участников исследования заявляют, что совет директоров принимает участие в рассмотрении текущих угроз информационной безопасности и защиты персональных данных, а это является важнейшим компонентом эффективной системы информационной безопасности.

Вместе с тем положение дел в этой области начинает меняться. Гэри Хейз (CenterPoint Energy) сообщил нам о том, что принимает участие в регулярных заседаниях ИТ-директоров 22 крупнейших коммунальных предприятий и что практически все они отчитываются перед советом директоров по вопросам безопасности.

И сам он поступает так же. По словам Хейза, он «отчитывается перед расширенным советом директоров два раза в год». Кроме того, он «на ежеквартальной основе представляет отчет комитету по аудиту». «Совет директоров недвусмысленно требует от нас предоставления информации о положении дел в этой области и о том, как мы реагируем на угрозы, потому что управление киберрисками поставлено в один ряд с наиболее серьезными задачами управления рисками предприятия», – разъясняет Хейз.

Рис. 10

В большинстве компаний совет директоров не участвует в ключевых мероприятиях по обеспечению информационной безопасности

Несмотря на прошлогодние нашумевшие инциденты в сфере нарушения безопасности, совет директоров зачастую не принимает участия в важнейших инициативах, таких как разработка стратегии безопасности, составление бюджета и анализ рисков.

06

Успешность отдельных инициатив в области информационной безопасности

Хотя мы обнаружили, что состояние дел в сфере применения некоторых практических методов обеспечения информационной безопасности ухудшилось, мы также отметили успехи, достигнутые в ряде важных областей.

Киберриски, технологии и уязвимости эволюционируют с молниеносной скоростью, и обмен информацией между государственными и частными компаниями о киберугрозах и принимаемых мерах становится основой эффективной программы кибербезопасности.

Для того чтобы повысить уровень своей безопасности и обеспечить более высокую эффективность работы по сбору и анализу информации об угрозах, организации все чаще начинают сотрудничать между собой и со сторонними организациями. По словам представителя компании CenterPoint г-на Хейза, его компания активно сотрудничает с рядом центров по анализу и обмену информацией (ISACs) и с отраслевыми ассоциациями, а также государственными органами. И эта инициатива уже доказала свою полезность.

«Если вы не можете участвовать в диалоге, то вы пропали, – говорит он. – При наличии столь серьезных угроз для безопасности отказываться от сотрудничества неразумно».

Участники исследования начинают осознавать пользу от совместной работы.

В этом году 55% опрошенных заявили, что идут на сотрудничество, чтобы повысить уровень своей безопасности, что на 12% больше, чем в 2013 году. Чем больше компания, тем выше вероятность того, что она станет сотрудничать с другими компаниями: так поступают 66% больших компаний и только 49% мелких фирм. Практика совместной работы получила наибольшее распространение в тех регионах, где в последние десять лет бурными темпами шло развитие ИТ-инфраструктуры. Так, например, респонденты из Южной Америки и Азиатско-Тихоокеанского региона с большей готовностью используют практику совместной работы, чтобы повысить эффективность своей деятельности по сбору и анализу разведданных в сфере безопасности.

В ситуации, когда смартфоны и планшеты становятся все более популярными, организации запаздывают с внедрением средств обеспечения безопасности, способных дать отпор мобильным угрозам. В этом году в данной области было отмечено заметное улучшение. Что касается самого базового уровня, то 54% респондентов утверждают, что внедрили в своих организациях стратегию мобильной безопасности. Принимая во внимание риски, связанные с мобильной средой, этот процент все еще нельзя назвать высоким, но это хороший результат по сравнению с 2013 годом, когда только у 42% респондентов существовала стратегия мобильной безопасности.

Для того чтобы обеспечить безопасность мобильных устройств, находящихся в собственности компаний и отдельных физических лиц, необходимы решения для управления мобильными устройствами (MDM) и мобильными приложениями (MAM). В этом году, согласно результатам исследования, решениями MDM/MAM пользуются уже 47% респондентов, что говорит об улучшении ситуации (для сравнения: в прошлом году этот показатель находился на уровне 39%). В то же время в этой области все еще сохраняется большой потенциал для улучшения.

Неудивительно, что большего прогресса в деле обеспечения мобильной безопасности удается добиться более крупным организациям, которые, как правило, реализуют более зрелые программы безопасности в целом. Самые высокие результаты с точки зрения совершенствования практики обеспечения мобильной безопасности показывают организации сектора финансовых услуг, компании индустрии телекоммуникаций и предприятия промышленного сектора.

В числе областей для улучшения можно назвать приобретение страховки в качестве инструмента по управлению киберрисками.

Как уже отмечалось выше, в США Управление инспекций и проверок соблюдения нормативно-правовых требований издало руководство, в котором организациям сектора финансовых услуг в рамках эффективной стратегии управления киберрисками рекомендуется оформлять киберстрахование. Мы полагаем, что с учетом нынешнего повышенного уровня угроз и роста материального ущерба от киберпреступности защита от финансовых потерь в результате киберрисков должна быть приравнена по значению к защите от других страхуемых рисков.

И похоже, что многие организации это понимают. Более половины (51%) респондентов утверждают, что приобрели страховку от киберрисков (для сравнения: 45% в 2013 году). Еще большее значение, возможно, имеет тот факт, что некоторые компании используют страхование от рисков киберпреступлений в качестве способа повышения эффективности своих программ безопасности. Более трети (36%) участников опроса приняли меры по укреплению своей безопасности, с тем чтобы снизить затраты на выплату страховых премий. Чаще всего страховку от киберрисков приобретают предприятия аэрокосмической и оборонной промышленности, автомобильной отрасли, компании индустрии развлечений, СМИ и организации финансового сектора.

Южная Америка лидирует в области страхования от киберрисков: соответствующий страховой полис в этом регионе приобрели **58%** респондентов. В США, где доля таких респондентов составила **44%**, инвестиции в страхование от киберрисков менее популярны.

07

От обеспечения безопасности к управлению киберрисками

По мере того как число инцидентов по всему миру продолжает стремительно расти, становится ясно, что киберриски никогда не будут полностью ликвидированы.

Сформировавшаяся в наши дни взаимозависимая экосистема бизнеса требует перехода от политики обеспечения информационной безопасности с акцентом на профилактике и контроле к подходу, основанному на оценке рисков, в рамках которого самые ценные активы организации и наиболее актуальные для нее угрозы будут ранжированы по приоритетности.

В этой связи крайне важно сосредоточить усилия на оперативном выявлении попыток несанкционированного доступа и разработать эффективные и своевременные ответные действия. Для решения этой задачи компаниям следует пересмотреть свои стратегии безопасности, обеспечив более тесную связь между такими компонентами, как технологии, процессы и квалифицированные кадры, с одной стороны, и деятельностью организации в области управления рисками в целом, с другой. По мнению Уильяма Бони (T-Mobile), многим компаниям это пока не по силам.

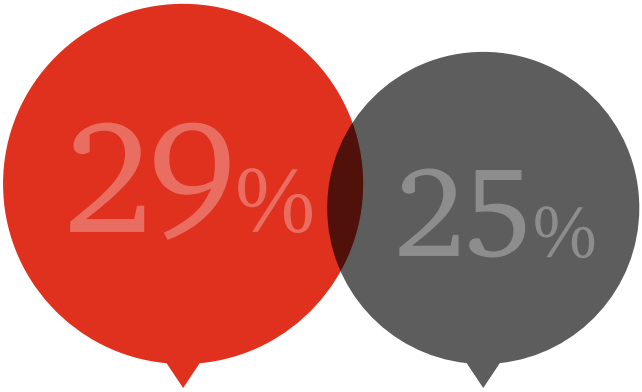
«Ситуации, когда у компаний имеются специалисты-практики и инструменты, необходимые для понимания проблем, связанных с обеспечением безопасности, и реагирования на них, а также руководители, способные разобраться в этих проблемах, встречаются редко, – отмечает Уильям Бони. – Очень многие все еще придерживаются той точки зрения, что проблема информационной безопасности лежит в сугубо технической плоскости, и считают, что для ее решения достаточно просто купить правильное программное обеспечение. А ведь информационная безопасность зависит от таких составляющих, как персонал, процессы и технологии. Умение задействовать все эти три элемента при разработке успешной программы безопасности в организации и найти их правильное сочетание является настоящим искусством».

Помимо прочего, это может помочь правильно распределять расходы на обеспечение информационной безопасности. «В вопросе о том, какую отдачу приносят вложения в безопасность, остается много неясностей. Компании зачастую не понимают, хорошо ли они справляются с поставленной задачей, – отмечает Бони. – Какой-либо общепринятой процедуры учета расходов на базовую кибербезопасность пока не разработано. Научиться говорить на одном языке и заложить основу для оценки компаниями эффективности своих инвестиций в информационную безопасность и соответствующих программ должен со временем помочь стандарт NIST».

Компаниям, желающим обеспечить сбалансированное использование трех ключевых компонентов (люди, процессы и технологии), следует обратить внимание на Концепцию кибербезопасности, разработанную NIST. Несмотря на то что этот документ ориентирован на организации, занимающиеся эксплуатацией объектов жизненно важной инфраструктуры в США, в нем содержится эффективная модель обеспечения безопасности на основе оценки рисков, которую могут взять на вооружение предприятия разной отраслевой направленности и географической принадлежности.

Мы полагаем, что эта программа стоит того, чтобы принять ее хотя бы ради заявленной в ней цели укрепления безопасности. Как отмечает представитель PwC Шон Джойс, принимавший участие в подготовке президентского указа с поручением разработать данную концепцию, «Концепция NIST – это яркий пример совместной работы государственного и частного секторов, в результате которой была разработана отличная универсальная концепция кибербезопасности».

Принятие этой концепции, помимо прочего, может принести дополнительные выгоды, среди которых можно отметить укрепление сотрудничества и повышение уровня информированности руководителей компаний и представителей отраслевых организаций о мерах по обеспечению безопасности. Этот шаг также позволит компаниям улучшить свои позиции с точки зрения риска судебных издержек в будущем, а также станет подспорьем в работе по обеспечению соответствия регулятивным требованиям[44].



Американские компании уже приступают к освоению Концепции NIST. **29%** респондентов из США утверждают, что они уже приняли Концепцию, а еще **25%** заявляют, что этот вопрос включен ими в список первоочередных задач на будущее.

Организации, участвовавшие в разработке Концепции NIST, как правило, в числе первых начинают следовать ее принципам. По словам Хейза, сотрудники компании CenterPoint параллельно созданию Концепции посещали семинары NIST и занимались разработкой плана реагирования на киберинциденты. После такого хорошего старта компания не стала затягивать с принятием и доработкой своего подхода, оптимально используя при этом Концепцию NIST. «Мы получили возможность усилить те аспекты кибербезопасности, которые, как нам кажется, имеют непосредственное отношение к нашей работе, – отмечает Хейз. – Мы использовали этот процесс, чтобы понять, что нам делать, и разработать план действий на будущее».

Согласно рекомендациям NIST, в первую очередь компаниям следует идентифицировать и классифицировать свои самые ценные информационные активы, а также определить, где в рамках экосистемы сосредоточены имеющие наибольшее значение данные и кто имеет к ним доступ.

Горнодобывающая компания Vale, предприняв эти первоначальные действия, смогла заложить прочный фундамент для своей программы информационной безопасности. «Прежде всего, мы разобрались с тем, какая информация относится к конфиденциальной, и определили, где она хранится, – рассказывает Фернандо Камаротти. – В результате мы получили важнейшую информацию о бизнес-аспектах информационной безопасности, а также поняли, как наши сотрудники используют конфиденциальные данные. Также эта работа помогла нам определить конкретные уровни защиты и понять, в каких областях можно допустить послабление, а в каких – действовать более жестко».

В то же время многие из участников нашего исследования пока еще не предприняли указанных шагов: программа выявления наиболее ценных информационных активов имеется только у 54% респондентов и всего лишь 56% приняли меры по инвентаризации способов сбора, передачи и хранения конфиденциальных данных сотрудников и клиентов. Такой стратегический подход к расходованию средств чаще всего используется предприятиями аэрокосмической и оборонной промышленности, компаниями сектора высоких технологий и сектора телекоммуникаций и организациями сектора финансовых услуг.

Если исходить из географического принципа, то можно сделать вывод о том, что респондентам из Южной Америки и Азиатско-Тихоокеанского региона более свойственно выделять средства из бюджета на безопасность и защиту своих самых ценных данных. Кроме того, большое значение имеет привязка стратегии безопасности к конкретным бизнес-потребностям, о чем забывают 40% респондентов. Среди отраслей, где стратегия безопасности чаще всего тесно связана с бизнес-стратегией, – промышленный сектор, сфера здравоохранения и медицинского страхования и сектор финансовых услуг. С точки зрения географии лидируют в этом направлении респонденты из Азиатско-Тихоокеанского региона и Северной Америки.

Следующий важнейший шаг – привязка бюджета на безопасность к стратегическим активам организации. Тем не менее **34%** респондентов не соотносят выделение средств из бюджета на безопасность с самыми доходными направлениями своей деятельности.

В рамках стратегического планирования расходов на безопасность компании, помимо прочего, должны определить, какие практические методы обеспечения кибербезопасности лучше всего подходят для реагирования на сегодняшние изощренные попытки несанкционированного доступа, и инвестировать именно в эти методы. Важно выделять средства на внедрение процессов, позволяющих полностью интегрировать средства прогнозирования, предотвращения, обнаружения и реагирования на инциденты, чтобы свести к минимуму их негативные последствия.

Кроме того, особое внимание следует уделять вложению достаточных средств в развитие кадрового потенциала и функциональности процессов, которые позволяют компаниям оперативно реагировать на инциденты и минимизировать их последствия. Юрист по вопросам кибербезопасности Лайза Сотто утверждает, что у многих из ее клиентов работа по повышению эффективности мер реагирования и минимизации отрицательных последствий инцидентов уже ведется. Помимо прочего, необходимо будет обеспечить достаточное финансирование полномасштабных курсов и программ непрерывного обучения сотрудников. Полезность обучения сотрудников в сфере безопасности подтверждают результаты Исследования по вопросам киберпреступности в США.

Компании, которые контролируют уровень осведомленности своих сотрудников в вопросах безопасности, средний уровень финансовых потерь от киберинцидентов ниже.

Экономия действительно может быть существенной: согласно полученным нами результатам, в компаниях, где не проводится обучение по вопросам безопасности для новых сотрудников, размер ежегодных финансовых потерь в четыре раза превышает аналогичный показатель в компаниях, где такое обучение организовано[45].

Чтобы максимально эффективно обеспечивать безопасность, необходимо иметь представление о существующих и потенциальных злоумышленниках, а также об их мотивах, ресурсах, которыми они располагают, и способах нападения. Эту задачу не решить без выделения средств на анализ и мониторинг угроз и без временных затрат и выделения ресурсов на сотрудничество с государственными учреждениями, правоохранительными органами, отраслевыми предприятиями и прочими третьими сторонами. Без этого достичь понимания ведущих методов обеспечения кибербезопасности невозможно. В нынешней ситуации стремительного нарастания внешних угроз методы обеспечения безопасности с учетом рисков должны стать основным компонентом имеющейся в организации общей системы управления рисками предприятия.

Лайза Сотто отмечает: «За период с декабря прошлого года к нам не раз обращались с просьбой помочь компаниям в совместной разработке программ упреждающих действий, направленных на минимизацию отрицательных последствий кибератаки, если она произойдет. До этого мы намного реже имели дело с таким видом действий на опережение».

Пусть тщательно продуманная программа управления киберрисками и не способна полностью устранить риск, однако она может помочь организациям управлять угрозами за счет принятия обоснованных решений, повысить эффективность средств обеспечения безопасности и создать более устойчивую к воздействию рисков систему безопасности.

Мы полагаем, что в ближайшие годы дальнейшие достижения в области компьютерных технологий научат организации лучше управлять рисками и последствиями киберугроз. Технологические прорывы должны помочь организациям снизить сложность задачи обеспечения кибербезопасности, увеличить скорость обнаружения инцидентов и устранения их последствий и повысить эффективность усилий по мониторингу и анализу деятельности в цифровом пространстве. А пока организации должны приложить усилия, чтобы лучше понять риски кибербезопасности, которые волнуют руководителей, членов советов директоров компаний и потребителей по всему миру, и научиться управлять этими рисками.

Методология

Глобальное исследование по вопросам обеспечения информационной безопасности за 2015 год (The Global State of Information Security®Survey 2015) – это всемирное исследование, проведенное фирмой PwC и журналами CIO и CSO.

Опрос проводился в онлайновом режиме с 27 марта по 25 мая 2014 года. Приглашения принять участие в исследовании были направлены по электронной почте читателям журналов CIO и CSO, а также клиентам PwC во всех регионах мира.

Если не указано иное, все цифры и графические данные, приведенные в настоящем отчете, основаны на результатах Глобального исследования по вопросам обеспечения информационной безопасности за 2015 год. Относительная погрешность составляет менее 1%.

В основе результатов, рассматриваемых в настоящем отчете, лежат ответы более чем 9 700 респондентов из 154 стран: руководителей компаний, финансовых директоров, директоров по информационной безопасности, директоров по информационным технологиям, руководителей служб безопасности, вице-президентов и директоров по вопросам информационных технологий и информационной безопасности.

Северная Америка

35%

Европа

34%

Азиатско-Тихоокеанский регион

14%

Южная Америка

13%

Африка и Ближний Восток

4%

Примечания, пояснения и источники

01
Киберриски: реальная и серьезная угроза

1 PwC, *The FBI says you've been breached by a nation-state. Now what?*, April 24, 2014

2 US Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014

3 BBC, *Wm Morrison supermarket suffers payroll data theft*, March 14, 2014

4 Symantec Corp., *Internet Security Threat Report 2014*, April 2014

5 TechWeek Europe, *Germany Investigating Data Breach Affecting 18 million*, April 7, 2014

6 Symantec Corp., *Turla: Spying tool targets governments and diplomats*, August 7, 2014

7 Cnet.com, *U.S. charges 8 in $45M global cybercrime scheme*, May 9, 2013

8 IOSCO and the World Federation of Exchanges Office, *Cyber-crime, securities markets and systemic risk*, July 2013

9 Department of Homeland Security, *ICS-CERT Monitor, January–April 2014*, May 2014

10 Financial Times, *Energy companies hit by cyber attack from Russia-linked group*, June 30, 2014

11 Ars Technica, *Critical crypto bug exposes Yahoo Mail, other passwords Russian roulette-style*, April 8, 2014

12 TrustedSec, *CHS Hacked via Heartbleed Vulnerability*, August 19, 2014

13 HP Fortify on Demand, *Internet of Things State of the Union Study*, July 2014

14 IOActive, *Adventures in Automotive Networks and Control Units*, August 2013

15 Securities and Exchange Commission, *National Exam Program Risk Alert*, April 15, 2014

16 Vormetric Data Security, *Security measures to go under spotlight as new Data Protection Directive approaches*, July 8, 2014

17 Singapore Personal Data Protection Commission, *Personal Data Protection Act Overview*, accessed August 23, 2014

18 Google Online Security Blog, *Announcing Project Zero*, July 15, 2014

19 The Wall Street Journal, *Global Security Spending to Grow 7.9% in 2014, Gartner Says*, August 22, 2014

20 The Wall Street Journal, *The Daily Startup: Venture Funding Soars for Cybersecurity Startups*, August 6, 2014

21 Quotes from wsj.com as of August 8, 2014

22 The Financial Times, *Europe's first cyber security-focused fund to launch*, June 18, 2014

23 TechCrunch, *Index Ventures Raises New $550M Early-Stage Fund For Europe, The US And Israel*, June 10, 2014

24 The Financial Times, *Investors flock to cyber security start-ups*, March 12, 2014

02
Число инцидентов и размеры причиняемого ими ущерба неуклонно растут

25 Trustwave Holdings, *2014 Trustwave Global Security Report*, May 2014

26 Center for Strategic and international Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, June 2014

27 Create.org and PwC, *Economic Impact of Trade Secret Theft*, February 2014

28 World Bank, *World Development Indicators Database*, July 2014; PwC calculations

29 World Economic Form, *Global Risks 2014, Ninth Edition*, December 2013

30 PwC, *Economic Crime: A threat to business globally*, February 2014

31 *2014 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

03
Сотрудники компаний чаще всего обвиняются в инцидентах

32 *2014 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

33 Verizon, *2014 Data Breach Investigations Report*, April 2014

34 The Financial Times, *Home Depot attack bigger than Target's*, September 19, 2014

35 Bureau of Justice Statistics, *Victims of Identity Theft*, 2012, December 2013

36 PwC, *Big Data: Big benefits and imperiled privacy*, June 2014

04
Число инцидентов растет, а расходы на обеспечение информационной безопасности сокращаются

37 PwC, *Economic Crime: A threat to business globally*, February 2014

38 PwC, *Fit for the future: Capitalizing on global trends*, April 2014

39 The Wall Street Journal, *Global Security Spending to Grow 7.9% in 2014, Gartner Says*, August 22, 2014

40 Booz & Co., *Highlights from the 2013 Global Innovation 1000 Study*, October 2013

41 Dell SecureWorks, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents, for over $1,000 Per Dossier*, July 15, 2013

42 RAND Corp., *Markets for Cybercrime Tools and Stolen Data*, 2014

05
Ухудшается положение в сфере применения основных практик обеспечения информационной безопасности

43 PwC, *16th Annual Global CEO Survey*, January 2013

07
От обеспечения безопасности к управлению киберрисками

44 PwC, *Why you should adopt the NIST Cybersecurity Framework*, May 2014

45 *2014 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

Контактная информация в разбивке по регионам

Австралия

Эндрю Гордон
Партнер
andrew.n.gordon@au.pwc.com

Стив Ингрэм
Партнер
steve.ingram@au.pwc.com

Бельгия

Флорис Ампе
Партнер
floris.ampe@be.pwc.com

Ближний Восток

Таха Хедро
Партнер
taha.khedro@ae.pwc.com

Ваддах Салах
Партнер
waddah.salah@sa.pwc.com

Бразилия

Эдгар Д'Андреа
Партнер
edgar.dandrea@br.pwc.com

Великобритания

Ричард Хорн
Партнер
richard.horne@uk.pwc.com

Грант Уотерфол
Партнер
grant.waterfall@uk.pwc.com

Германия

Дерк Фишер
Партнер
derk.fischer@de.pwc.com

Вильфрид Мейер
Партнер
wilfried.meyer@de.pwc.com

Дания

Кристиан Кьяэр
Директор
christian.x.kjaer@dk.pwc.com

Мадс Норгаард Мадсен
Директор
mads.norgaard.madsen@dk.pwc.com

Израиль

Ярон Блахман
Партнер
yaron.blachman@il.pwc.com

Индия

Сиварама Кришнан
Партнер
sivarama.krishnan@in.pwc.com

Испания

Елена Маэстре
Партнер
elena.maestre@es.pwc.com

Хавьер Уртьяга Баонса
Партнер
javier.urtiaga@es.pwc.com

Италия

Фабио Мерелло
Партнер
fabio.merello@it.pwc.com

Канада

Салим Хашам
Партнер
s.hasham@ca.pwc.com

Китай

Рамеш Муса
Партнер
ramesh.moosa@cn.pwc.com

Кеннет Вонг
Партнер
kenneth.ks.wong@hk.pwc.com

Нидерланды

Эрвин де Хорд
Партнер
erwin.de.horde@nl.pwc.com

Гервин Набер
Партнер
gerwin.naber@nl.pwc.com

Отто Вермюлен
Партнер
otto.vermeulen@nl.pwc.com

Новая Зеландия

Адриан Ван Хест
Партнер
adrian.p.van.hest@nz.pwc.com

Норвегия

Том Ремберг
Директор
tom.remberg@no.pwc.com

Польша

Рафал Ячински
Директор
rafal.jaczynski@pl.pwc.com

Петр Урбан
Партнер
piotr.urban@pl.pwc.com

Россия

Кристофер Гоулд
Партнер
chirstopher.gould@ru.pwc.com

Сингапур

Винсент Лой
Партнер
vincent.j.loy@sg.pwc.com

Кок Венг Сам
Партнер
kok.weng.sam@sg.pwc.com

США

Дэвид Берг
Директор
david.b.burg@us.pwc.com

Шон Джойс
Директор
sean.joyce@us.pwc.com

Марк Лобел
Директор
mark.a.lobel@us.pwc.com

Турция

Бурак Садик
Старший менеджер
burak.sadic@tr.pwc.com

Франция

Филипп Трушо
Партнер
philippe.trouchaud@fr.pwc.com

Швейцария

Томас Кох
Директор
thomas.koch@ch.pwc.com

Ян Шрудер
Партнер
jan.schreuder@ch.pwc.com

Швеция

Эмиль Гуллерс
Партнер
emil.gullers@se.pwc.com

Якоб Хенриксон
Партнер
jacob.henricson@se.pwc.com

ЮАР

Пьер Далтон
Партнер
pierre.dalton@za.pwc.com

Марк Телфер
Партнер
mark.telfer@za.pwc.com

Сидрианн де Виллиерс
Партнер
sidriann.de.villiers@za.pwc.com

Южная Корея

Сунг Бэ Чо
Директор
sung-bae.cho@kr.pwc.com

Чжэ Хен Чжу
Партнер
jae-hyeong.joo@kr.pwc.com

Япония

Маки Мацудзаки
Партнер
maki.matsuzaki@jp.pwc.com

Наоки Ямамото
Директор
naoki.n.yamamoto@jp.pwc.com

Контакты

Крис Гулд

Партнер
Отдел анализа и контроля рисков
Тел.: + 7 (495) 967 6368
christopher.gould@ru.pwc.com

Роман Чаплыгин

Директор
Отдел анализа и контроля рисков
Тел.: +7 (495) 967 6056
roman.chaplygin@ru.pwc.com

www.pwc.com/gsiss2015
www.pwc.ru/cybersecurity

1177